

Table 0.1 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1) \xrightarrow{1r} (1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,0)$	16,17,18	17,18	$2^{-17.5}$
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0) \xrightarrow{1r} (1,1,0,0,0,0,0,0,1,0,0,0,0,0,0,0)$	18	15,18	2^{-1}
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1) \xrightarrow{1r} (0,0,1,1,1,1,1,0,1,1,1,1,1,1,1,0)$	16,17	15,17	$2^{-17.5}$
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0) \xrightarrow{1r} (1,1,0,1,1,1,0,1,0,1,1,1,1,1,1,1)$	14,17,18	17,18	$2^{-17.5}$
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,1) \xrightarrow{1r} (0,0,1,0,0,0,1,0,1,0,0,0,0,0,0,1)$	14,16	—	2^{-12}
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,0) \xrightarrow{1r} (0,0,0,1,1,1,0,0,0,1,1,1,1,1,1,1)$	14,17	15,17	$2^{-17.5}$
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,1) \xrightarrow{1r} (1,1,1,0,0,0,1,1,1,0,0,0,0,0,0,1)$	14,16,18	15,18	2^{-12}
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0) \xrightarrow{1r} (1,1,0,1,0,1,0,0,0,1,0,0,0,0,0,0)$	18	13,18	$2^{-6.5}$
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,1) \xrightarrow{1r} (0,0,1,0,1,0,1,1,1,0,1,1,1,1,1,0)$	16,17	13,17	2^{-23}
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,1,0) \xrightarrow{1r} (0,0,0,1,0,1,0,1,0,1,0,1,0,0,0,0,0,0)$	—	13,15	$2^{-6.5}$
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,1,1) \xrightarrow{1r} (1,1,1,0,1,0,1,0,1,0,1,0,1,1,1,1,0)$	16,17,18	13,15,17,18	2^{-23}
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,0,0) \xrightarrow{1r} (0,0,0,0,1,0,0,1,0,0,1,1,1,1,1,1,1)$	14,17	13,17	2^{-12}
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,0,1) \xrightarrow{1r} (1,1,1,1,0,1,1,0,1,1,0,0,0,0,0,0,1)$	14,16,18	13,18	$2^{-6.5}$
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,0) \xrightarrow{1r} (1,1,0,0,1,0,0,0,0,0,0,0,1,1,1,1,1,1)$	14,17,18	13,15,17,18	2^{-12}
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,1) \xrightarrow{1r} (0,0,1,1,0,1,1,1,1,1,0,0,0,0,0,0,1)$	14,16	13,15	$2^{-6.5}$
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0) \xrightarrow{1r} (1,1,0,1,1,1,1,1,0,1,0,1,1,1,1,1,1)$	12,17,18	17,18	$2^{-17.5}$
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,1) \xrightarrow{1r} (0,0,1,0,0,0,0,0,1,0,1,0,0,0,0,0,1)$	12,16	—	2^{-23}
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,1,0) \xrightarrow{1r} (0,0,0,1,1,1,1,0,0,1,0,1,1,1,1,1,1)$	12,17	15,17	$2^{-17.5}$
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,1,1) \xrightarrow{1r} (1,1,1,0,0,0,0,1,1,0,1,0,0,0,0,0,1)$	12,16,18	15,18	2^{-23}
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,1,0,0) \xrightarrow{1r} (0,0,0,0,0,0,1,0,0,0,1,0,0,0,0,0,0)$	12,14	—	2^{-12}
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,1,0,1) \xrightarrow{1r} (1,1,1,1,1,1,0,1,1,1,0,1,1,1,1,1,0)$	12,14,16,17,18	17,18	$2^{-17.5}$
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,1,1,0) \xrightarrow{1r} (1,1,0,0,0,0,1,1,0,0,1,0,0,0,0,0,0)$	12,14,18	15,18	2^{-12}
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,1,1,1) \xrightarrow{1r} (0,0,1,1,1,1,0,0,1,1,0,1,1,1,1,1,0)$	12,14,16,17	15,17	$2^{-17.5}$
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,0,0,0) \xrightarrow{1r} (0,0,0,0,1,0,1,1,0,0,0,0,1,1,1,1,1)$	12,17	13,17	2^{-12}
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,0,0,1) \xrightarrow{1r} (1,1,1,1,0,1,0,0,1,1,1,1,0,0,0,0,1)$	12,16,18	13,18	$2^{-17.5}$
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,0,1,0) \xrightarrow{1r} (1,1,0,0,1,0,1,0,0,0,0,0,1,1,1,1,1)$	12,17,18	13,15,17,18	2^{-12}
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,0,1,1) \xrightarrow{1r} (0,0,1,1,0,1,0,1,1,1,1,1,0,0,0,0,1)$	12,16	13,15	$2^{-17.5}$
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,0,0) \xrightarrow{1r} (1,1,0,1,0,1,1,0,0,1,1,0,0,0,0,0,0)$	12,14,18	13,18	$2^{-17.5}$
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,0,1) \xrightarrow{1r} (0,0,1,0,1,0,0,1,1,0,0,1,1,1,1,1,0)$	12,14,16,17	13,17	2^{-23}
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,1,0) \xrightarrow{1r} (0,0,0,1,0,1,1,1,0,1,1,0,0,1,1,1,1,0)$	12,14	13,15	$2^{-17.5}$
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,1,1) \xrightarrow{1r} (1,1,1,0,1,0,0,0,1,0,0,1,1,1,1,1,0)$	12,14,16,17,18	13,15,17,18	2^{-23}

Table 0.2 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (1,1,0,0,0,1,0,0,0,1,0,1,0,0,0,0,0,0)$	18	11,18	2^{-12}
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (0,0,1,1,1,0,1,1,1,0,1,0,1,1,1,0,0,0)$	16,17	11,17	$2^{-28.5}$
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (0,0,0,0,0,1,0,1,0,1,0,1,0,0,0,0,0,0)$	—	11,15	2^{-12}
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (1,1,1,1,1,0,1,0,1,0,1,0,1,1,1,0,0,0)$	16,17,18	11,15,17,18	$2^{-28.5}$
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (0,0,0,1,1,0,0,1,0,0,1,0,1,1,1,1,0,0)$	14,17	11,17	$2^{-17.5}$
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (1,1,1,0,0,1,1,0,1,1,0,1,0,0,0,0,0,0)$	14,16,18	11,18	2^{-12}
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (1,1,0,1,1,0,0,0,0,0,0,1,0,1,1,1,1,0)$	14,17,18	11,15,17,18	$2^{-17.5}$
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (0,0,1,0,0,1,1,1,1,0,1,0,0,0,0,0,0,0)$	14,16	11,15	2^{-12}
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (0,0,0,1,0,0,0,0,0,0,0,0,0,1,0,0,0,0)$	—	11,13	$2^{-6.5}$
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (1,1,1,0,1,1,1,1,1,1,1,0,1,1,1,0,0,0)$	16,17,18	11,13,17,18	2^{-23}
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (1,1,0,1,0,0,0,1,0,0,0,1,0,0,0,0,0,0)$	18	11,13,15,18	$2^{-6.5}$
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (0,0,1,0,1,1,1,0,1,1,1,0,1,1,1,0,0,0)$	16,17	11,13,15,17	2^{-23}
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (1,1,0,0,1,1,0,1,0,1,0,1,1,0,1,1,1,0)$	14,17,18	11,13,17,18	2^{-23}
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (0,0,1,1,0,0,1,0,1,0,0,1,0,0,0,0,0,0)$	14,16	11,13	$2^{-17.5}$
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (0,0,0,0,1,1,0,0,0,1,1,0,1,1,1,1,0,0)$	14,17	11,13,15,17	2^{-23}
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (1,1,1,1,0,0,1,1,1,0,0,1,0,0,0,0,0,0)$	14,16,18	11,13,15,18	$2^{-17.5}$
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (0,0,0,1,1,0,1,1,0,0,0,0,1,1,1,1,0,0)$	12,17	11,17	$2^{-6.5}$
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (1,1,1,0,0,1,0,0,1,1,1,1,0,0,0,0,0,0)$	12,16,18	11,18	2^{-12}
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (1,1,0,1,1,0,1,0,0,0,0,0,0,1,1,1,1,0)$	12,17,18	11,15,17,18	$2^{-6.5}$
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (0,0,1,0,0,1,0,1,1,1,1,1,0,0,0,0,0,0)$	12,16	11,15	2^{-12}
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (1,1,0,0,0,1,1,0,0,1,1,1,0,0,0,0,0,0)$	12,14,18	11,18	2^{-12}
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (0,0,1,1,1,0,0,1,1,0,0,0,1,1,1,0,0,0)$	12,14,16,17	11,17	$2^{-17.5}$
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (0,0,0,0,0,1,1,1,0,1,1,1,0,0,0,0,0,0)$	12,14	11,15	2^{-12}
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (1,1,1,1,1,0,0,0,1,0,0,0,1,1,1,0,0,0)$	12,14,16,17,18	11,15,17,18	$2^{-17.5}$
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (1,1,0,0,1,1,1,1,0,1,0,0,1,1,1,1,0,0)$	12,17,18	11,13,17,18	2^{-12}
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (0,0,1,1,0,0,0,0,1,0,1,1,0,0,0,0,0,0)$	12,16	11,13	$2^{-17.5}$
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (0,0,0,0,1,1,1,0,0,1,0,0,1,1,1,1,0,0)$	12,17	11,13,15,17	2^{-12}
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (1,1,1,1,0,0,0,1,1,0,1,1,0,0,0,0,0,0)$	12,16,18	11,13,15,18	$2^{-17.5}$
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (0,0,0,1,0,0,1,0,0,0,0,1,1,0,0,0,0,0)$	12,14	11,13	$2^{-6.5}$
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (1,1,1,0,1,1,0,1,1,1,0,0,1,1,1,0,0,0)$	12,14,16,17,18	11,13,17,18	2^{-12}
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (1,1,0,1,0,0,1,1,0,0,1,1,0,0,0,0,0,0)$	12,14,18	11,13,15,18	$2^{-6.5}$
$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (0,0,1,0,1,1,0,0,1,1,0,0,1,1,1,0,0,0)$	12,14,16,17	11,13,15,17	2^{-12}

Table 0.3 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0) \xrightarrow{1r} (1,1,1,1,0,1,0,1,0,1,0,1,0,1,1,1)$	10,17,18	17,18	$2^{-17.5}$
$(0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,1) \xrightarrow{1r} (0,0,0,0,1,0,1,0,1,0,1,0,1,0,0,1)$	10,16	—	2^{-34}
$(0,0,0,0,0,0,0,0,0,1,0,0,0,0,1,0) \xrightarrow{1r} (0,0,1,1,0,1,0,0,0,1,0,1,0,1,1,1)$	10,17	15,17	$2^{-17.5}$
$(0,0,0,0,0,0,0,0,0,1,0,0,0,0,1,1) \xrightarrow{1r} (1,1,0,0,1,0,1,1,1,0,1,0,1,0,0,1)$	10,16,18	15,18	2^{-34}
$(0,0,0,0,0,0,0,0,0,1,0,0,0,1,0,0) \xrightarrow{1r} (0,0,1,0,1,0,0,0,0,0,1,0,1,0,0,0)$	10,14	—	2^{-23}
$(0,0,0,0,0,0,0,0,0,1,0,0,0,1,0,1) \xrightarrow{1r} (1,1,0,1,0,1,1,1,1,0,1,0,1,1,0,0)$	10,14,16,17,18	17,18	$2^{-17.5}$
$(0,0,0,0,0,0,0,0,0,1,0,0,0,1,1,0) \xrightarrow{1r} (1,1,1,0,1,0,0,1,0,0,1,0,1,0,0,0)$	10,14,18	15,18	2^{-23}
$(0,0,0,0,0,0,0,0,0,1,0,0,0,1,1,1) \xrightarrow{1r} (0,0,0,1,0,1,1,0,1,1,0,1,0,1,1,0)$	10,14,16,17	15,17	$2^{-17.5}$
$(0,0,0,0,0,0,0,0,0,1,0,0,1,0,0,0) \xrightarrow{1r} (0,0,1,0,0,0,0,1,0,0,0,1,0,1,1,1)$	10,17	13,17	2^{-12}
$(0,0,0,0,0,0,0,0,0,1,0,0,1,0,0,1) \xrightarrow{1r} (1,1,0,1,1,1,0,1,1,1,0,1,0,1,0,0,1)$	10,16,18	13,18	$2^{-28.5}$
$(0,0,0,0,0,0,0,0,0,1,0,0,1,0,1,0) \xrightarrow{1r} (1,1,1,0,0,0,0,0,0,0,0,0,1,0,1,1,1)$	10,17,18	13,15,17,18	2^{-12}
$(0,0,0,0,0,0,0,0,0,1,0,0,1,0,1,1) \xrightarrow{1r} (0,0,0,1,1,1,1,1,1,1,1,0,1,0,0,1)$	10,16	13,15	$2^{-28.5}$
$(0,0,0,0,0,0,0,0,0,1,0,0,1,1,0,0) \xrightarrow{1r} (1,1,1,1,1,1,0,0,0,1,1,0,1,0,0,0)$	10,14,18	13,18	$2^{-28.5}$
$(0,0,0,0,0,0,0,0,0,1,0,0,1,1,0,1) \xrightarrow{1r} (0,0,0,0,0,0,1,1,1,0,0,1,0,1,1,0)$	10,14,16,17	13,17	2^{-23}
$(0,0,0,0,0,0,0,0,0,1,0,0,1,1,1,0) \xrightarrow{1r} (0,0,1,1,1,1,0,1,0,1,1,0,1,0,0,0)$	10,14	13,15	$2^{-28.5}$
$(0,0,0,0,0,0,0,0,0,1,0,0,1,1,1,1) \xrightarrow{1r} (1,1,0,0,0,0,1,0,1,0,0,1,0,1,1,0)$	10,14,16,17,18	13,15,17,18	2^{-23}
$(0,0,0,0,0,0,0,0,0,1,0,1,0,0,0,0) \xrightarrow{1r} (0,0,1,0,1,0,1,0,0,0,0,0,1,0,0,0)$	10,12	—	2^{-12}
$(0,0,0,0,0,0,0,0,0,1,0,1,0,0,0,1) \xrightarrow{1r} (1,1,0,1,0,1,0,1,1,1,1,0,1,1,0,1)$	10,12,16,17,18	17,18	$2^{-17.5}$
$(0,0,0,0,0,0,0,0,0,1,0,1,0,0,1,0) \xrightarrow{1r} (1,1,1,0,1,0,1,1,0,0,0,0,1,0,0,0)$	10,12,18	15,18	2^{-12}
$(0,0,0,0,0,0,0,0,0,1,0,1,0,0,1,1) \xrightarrow{1r} (0,0,0,1,0,1,0,0,1,1,1,1,0,1,1,0)$	10,12,16,17	15,17	$2^{-17.5}$
$(0,0,0,0,0,0,0,0,0,1,0,1,0,1,0,0) \xrightarrow{1r} (1,1,1,1,0,1,1,1,0,1,1,1,0,1,1,1)$	10,12,14,17,18	17,18	$2^{-17.5}$
$(0,0,0,0,0,0,0,0,0,1,0,1,0,1,0,1) \xrightarrow{1r} (0,0,0,0,1,0,0,0,1,0,0,0,1,0,0,1)$	10,12,14,16	—	2^{-23}
$(0,0,0,0,0,0,0,0,0,1,0,1,0,1,1,0) \xrightarrow{1r} (0,0,1,1,0,1,1,0,0,1,1,1,0,1,1,1)$	10,12,14,17	15,17	$2^{-17.5}$
$(0,0,0,0,0,0,0,0,0,1,0,1,0,1,1,1) \xrightarrow{1r} (1,1,0,0,1,0,0,1,1,0,0,0,1,0,0,1)$	10,12,14,16,18	15,18	2^{-23}
$(0,0,0,0,0,0,0,0,0,1,0,1,1,0,0,0) \xrightarrow{1r} (1,1,1,1,1,1,1,0,0,1,0,0,1,0,0,0)$	10,12,18	13,18	$2^{-17.5}$
$(0,0,0,0,0,0,0,0,0,1,0,1,1,0,0,1) \xrightarrow{1r} (0,0,0,0,0,0,0,1,1,0,1,1,0,1,1,0)$	10,12,16,17	13,17	2^{-23}
$(0,0,0,0,0,0,0,0,0,1,0,1,1,0,1,0) \xrightarrow{1r} (0,0,1,1,1,1,1,1,0,1,0,0,1,0,0,0)$	10,12	13,15	$2^{-17.5}$
$(0,0,0,0,0,0,0,0,0,1,0,1,1,0,1,1) \xrightarrow{1r} (1,1,0,0,0,0,0,0,1,0,1,1,0,1,1,0)$	10,12,16,17,18	13,15,17,18	2^{-23}
$(0,0,0,0,0,0,0,0,0,1,0,1,1,1,0,0) \xrightarrow{1r} (0,0,1,0,0,0,1,1,0,0,1,1,0,1,1,1)$	10,12,14,17	13,17	2^{-12}
$(0,0,0,0,0,0,0,0,0,1,0,1,1,1,0,1) \xrightarrow{1r} (1,1,0,1,1,1,0,0,1,1,0,0,1,0,0,1)$	10,12,14,16,18	13,18	$2^{-17.5}$
$(0,0,0,0,0,0,0,0,0,1,0,1,1,1,1,0) \xrightarrow{1r} (1,1,1,0,0,0,1,0,0,0,1,1,0,1,1,1)$	10,12,14,17,18	13,15,17,18	2^{-12}
$(0,0,0,0,0,0,0,0,0,1,0,1,1,1,1,1) \xrightarrow{1r} (0,0,0,1,1,1,0,1,1,1,0,0,1,0,0,1)$	10,12,14,16	13,15	$2^{-17.5}$

Table 0.4 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	10,17	11,17	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	10,16,18	11,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	10,17,18	11,15,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	10,16	11,15	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	10,14,18	11,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	10,14,16,17	11,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	10,14	11,15	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	10,14,16,17,18	11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	10,17,18	11,13,17,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	10,16	11,13	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	10,17	11,13,15,17	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	10,16,18	11,13,15,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	10,14	11,13	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	10,14,16,17,18	11,13,17,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	10,14,18	11,13,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	10,14,16,17	11,13,15,17	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	10,12,18	11,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	10,12,16,17	11,17	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	10,12	11,15	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	10,12,16,17,18	11,15,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	10,12,14,17	11,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	10,12,14,16,18	11,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	10,12,14,17,18	11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	10,12,14,16	11,15	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	10,12	11,13	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	10,12,16,17,18	11,13,17,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	10,12,18	11,13,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	10,12,16,17	11,13,15,17	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	10,12,14,17,18	11,13,17,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	10,12,14,16	11,13	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	10,12,14,17	11,13,15,17	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	10,12,14,16,18	11,13,15,18	$2^{-28.5}$

Table 0.5 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	18	9,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	16,17	9,17	2^{-34}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	—	9,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	16,17,18	9,15,17,18	2^{-34}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	14,17	9,17	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	14,16,18	9,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	14,17,18	9,15,17,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	14,16	9,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	—	9,13	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	16,17,18	9,13,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	18	9,13,15,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	16,17	9,13,15,17	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	14,17,18	9,13,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	14,16	9,13	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	14,17	9,13,15,17	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	14,16,18	9,13,15,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	12,17	9,17	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	12,16,18	9,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	12,17,18	9,15,17,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	12,16	9,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	12,14,18	9,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	12,14,16,17	9,17	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	12,14	9,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	12,14,16,17,18	9,15,17,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	12,17,18	9,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	12,16	9,13	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	12,17	9,13,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	12,16,18	9,13,15,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	12,14	9,13	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	12,14,16,17,18	9,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	12,14,18	9,13,15,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	12,14,16,17	9,13,15,17	$2^{-17.5}$

Table 0.6 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	—	9,11	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	16,17,18	9,11,17,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	18	9,11,15,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	16,17	9,11,15,17	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	14,17,18	9,11,17,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	14,16	9,11	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	14,17	9,11,15,17	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	14,16,18	9,11,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	18	9,11,13,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	16,17	9,11,13,17	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	—	9,11,13,15	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	16,17,18	9,11,13,15,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	14,17	9,11,13,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	14,16,18	9,11,13,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	14,17,18	9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	14,16	9,11,13,15	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	12,17,18	9,11,17,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	12,16	9,11	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	12,17	9,11,15,17	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	12,16,18	9,11,15,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	12,14	9,11	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	12,14,16,17,18	9,11,17,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	12,14,18	9,11,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	12,14,16,17	9,11,15,17	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	12,17	9,11,13,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	12,16,18	9,11,13,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	12,17,18	9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	12,16	9,11,13,15	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	12,14,18	9,11,13,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	12,14,16,17	9,11,13,17	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	12,14	9,11,13,15	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	12,14,16,17,18	9,11,13,15,17,18	$2^{-28.5}$

Table 0.7 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	10,17	9,17	2^{-1}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	10,16,18	9,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	10,17,18	9,15,17,18	2^{-1}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	10,16	9,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	10,14,18	9,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	10,14,16,17	9,17	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	10,14	9,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	10,14,16,17,18	9,15,17,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	10,17,18	9,13,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	10,16	9,13	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	10,17	9,13,15,17	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	10,16,18	9,13,15,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	10,14	9,13	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	10,14,16,17,18	9,13,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	10,14,18	9,13,15,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	10,14,16,17	9,13,15,17	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	10,12,18	9,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	10,12,16,17	9,17	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	10,12	9,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	10,12,16,17,18	9,15,17,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	10,12,14,17	9,17	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	10,12,14,16,18	9,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	10,12,14,17,18	9,15,17,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	10,12,14,16	9,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	10,12	9,13	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	10,12,16,17,18	9,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	10,12,18	9,13,15,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	10,12,16,17	9,13,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	10,12,14,17,18	9,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	10,12,14,16	9,13	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	10,12,14,17	9,13,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	10,12,14,16,18	9,13,15,18	2^{-23}

Table 0.8 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	10,17,18	9,11,17,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	10,16	9,11	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	10,17	9,11,15,17	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	10,16,18	9,11,15,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	10,14	9,11	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	10,14,16,17,18	9,11,17,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	10,14,18	9,11,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	10,14,16,17	9,11,15,17	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	10,17	9,11,13,17	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	10,16,18	9,11,13,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	10,17,18	9,11,13,15,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	10,16	9,11,13,15	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	10,14,18	9,11,13,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	10,14,16,17	9,11,13,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	10,14	9,11,13,15	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	10,14,16,17,18	9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	10,12	9,11	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	10,12,16,17,18	9,11,17,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	10,12,18	9,11,15,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	10,12,16,17	9,11,15,17	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	10,12,14,17,18	9,11,17,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	10,12,14,16	9,11	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	10,12,14,17	9,11,15,17	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	10,12,14,16,18	9,11,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	10,12,18	9,11,13,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	10,12,16,17	9,11,13,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	10,12	9,11,13,15	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	10,12,16,17,18	9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	10,12,14,17	9,11,13,17	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	10,12,14,16,18	9,11,13,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	10,12,14,17,18	9,11,13,15,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	10,12,14,16	9,11,13,15	2^{-12}

Table 0.9 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	17,18	8,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	16	8	2^{-1}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	17	8,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	16,18	8,15,18	2^{-1}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	14	8	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	14,16,17,18	8,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	14,18	8,15,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	14,16,17	8,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	17	8,13,17	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	16,18	8,13,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	17,18	8,13,15,17,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	16	8,13,15	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	14,18	8,13,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	14,16,17	8,13,17	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	14	8,13,15	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	14,16,17,18	8,13,15,17,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	12	8	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	12,16,17,18	8,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	12,18	8,15,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	12,16,17	8,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	12,14,17,18	8,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	12,14,16	8	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	12,14,17	8,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	12,14,16,18	8,15,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	12,18	8,13,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	12,16,17	8,13,17	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	12	8,13,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	12,16,17,18	8,13,15,17,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	12,14,17	8,13,17	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	12,14,16,18	8,13,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	12,14,17,18	8,13,15,17,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	12,14,16	8,13,15	$2^{-17.5}$

Table 0.10 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	17	8,11,17	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	16,18	8,11,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	17,18	8,11,15,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	16	8,11,15	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	14,18	8,11,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	14,16,17	8,11,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	14	8,11,15	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	14,16,17,18	8,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	17,18	8,11,13,17,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	16	8,11,13	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	17	8,11,13,15,17	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	16,18	8,11,13,15,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	14	8,11,13	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	14,16,17,18	8,11,13,17,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	14,18	8,11,13,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	14,16,17	8,11,13,15,17	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	12,18	8,11,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	12,16,17	8,11,17	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	12	8,11,15	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	12,16,17,18	8,11,15,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	12,14,17	8,11,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	12,14,16,18	8,11,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	12,14,17,18	8,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	12,14,16	8,11,15	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	12	8,11,13	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	12,16,17,18	8,11,13,17,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	12,18	8,11,13,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	12,16,17	8,11,13,15,17	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	12,14,17,18	8,11,13,17,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	12,14,16	8,11,13	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	12,14,17	8,11,13,15,17	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	12,14,16,18	8,11,13,15,18	$2^{-6.5}$

Table 0.11 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	10	8	2^{-34}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	10,16,17,18	8,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	10,18	8,15,18	2^{-34}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	10,16,17	8,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	10,14,17,18	8,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	10,14,16	8	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	10,14,17	8,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	10,14,16,18	8,15,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	10,18	8,13,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	10,16,17	8,13,17	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	10	8,13,15	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	10,16,17,18	8,13,15,17,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	10,14,17	8,13,17	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	10,14,16,18	8,13,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	10,14,17,18	8,13,15,17,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	10,14,16	8,13,15	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	10,12,17,18	8,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	10,12,16	8	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	10,12,17	8,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	10,12,16,18	8,15,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	10,12,14	8	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	10,12,14,16,17,18	8,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	10,12,14,18	8,15,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	10,12,14,16,17	8,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	10,12,17	8,13,17	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	10,12,16,18	8,13,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	10,12,17,18	8,13,15,17,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	10,12,16	8,13,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	10,12,14,18	8,13,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	10,12,14,16,17	8,13,17	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	10,12,14	8,13,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	10,12,14,16,17,18	8,13,15,17,18	2^{-12}

Table 0.12 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	10,18	8,11,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	10,16,17	8,11,17	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	10	8,11,15	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	10,16,17,18	8,11,15,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	10,14,17	8,11,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	10,14,16,18	8,11,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	10,14,17,18	8,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	10,14,16	8,11,15	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	10	8,11,13	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	10,16,17,18	8,11,13,17,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	10,18	8,11,13,15,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	10,16,17	8,11,13,15,17	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	10,14,17,18	8,11,13,17,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	10,14,16	8,11,13	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	10,14,17	8,11,13,15,17	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	10,14,16,18	8,11,13,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	10,12,17	8,11,17	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	10,12,16,18	8,11,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	10,12,17,18	8,11,15,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	10,12,16	8,11,15	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	10,12,14,18	8,11,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	10,12,14,16,17	8,11,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	10,12,14	8,11,15	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	10,12,14,16,17,18	8,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	10,12,17,18	8,11,13,17,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	10,12,16	8,11,13	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	10,12,17	8,11,13,15,17	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	10,12,16,18	8,11,13,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	10,12,14	8,11,13	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	10,12,14,16,17,18	8,11,13,17,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	10,12,14,18	8,11,13,15,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	10,12,14,16,17	8,11,13,15,17	2^{-23}

Table 0.13 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,0,0,0,1,1,0,0,0,0,0,0,0) \xrightarrow{1r} (0,1,1,0,1,0,1,0,1,0,1,0,1,0,0,1)$	17	8,9,17	2^{-34}
$(0,0,0,0,0,0,0,1,1,0,0,0,0,0,0,1) \xrightarrow{1r} (1,0,0,1,0,1,0,1,0,1,0,1,0,1,1,1)$	16,18	8,9,18	$2^{-17.5}$
$(0,0,0,0,0,0,0,1,1,0,0,0,0,0,1,0) \xrightarrow{1r} (1,0,1,0,1,0,1,1,1,0,1,0,1,0,0,1)$	17,18	8,9,15,17,18	2^{-34}
$(0,0,0,0,0,0,0,1,1,0,0,0,0,0,1,1) \xrightarrow{1r} (0,1,0,1,0,1,0,0,0,1,0,1,0,1,1,1)$	16	8,9,15	$2^{-17.5}$
$(0,0,0,0,0,0,0,1,1,0,0,0,0,1,0,0) \xrightarrow{1r} (1,0,1,1,0,1,1,1,1,1,0,1,0,1,1,0)$	14,18	8,9,18	$2^{-17.5}$
$(0,0,0,0,0,0,0,1,1,0,0,0,0,1,0,1) \xrightarrow{1r} (0,1,0,0,1,0,0,0,0,0,1,0,1,0,0,0)$	14,16,17	8,9,17	2^{-23}
$(0,0,0,0,0,0,0,1,1,0,0,0,0,1,1,0) \xrightarrow{1r} (0,1,1,1,0,1,1,0,1,1,0,1,0,1,1,0)$	14	8,9,15	$2^{-17.5}$
$(0,0,0,0,0,0,0,1,1,0,0,0,0,1,1,1) \xrightarrow{1r} (1,0,0,0,1,0,0,1,0,0,1,0,1,0,0,0)$	14,16,17,18	8,9,15,17,18	2^{-23}
$(0,0,0,0,0,0,0,1,1,0,0,0,1,0,0,0) \xrightarrow{1r} (1,0,1,1,1,1,1,0,1,1,1,0,1,0,0,1)$	17,18	8,9,13,17,18	$2^{-28.5}$
$(0,0,0,0,0,0,0,1,1,0,0,0,1,0,0,1) \xrightarrow{1r} (0,1,0,0,0,0,0,1,0,0,0,1,0,1,1,1)$	16	8,9,13	2^{-12}
$(0,0,0,0,0,0,0,1,1,0,0,0,1,0,1,0) \xrightarrow{1r} (0,1,1,1,1,1,1,1,1,1,0,1,0,0,1)$	17	8,9,13,15,17	$2^{-28.5}$
$(0,0,0,0,0,0,0,1,1,0,0,0,1,0,1,1) \xrightarrow{1r} (1,0,0,0,0,0,0,0,0,0,0,1,0,1,1,1)$	16,18	8,9,13,15,18	2^{-12}
$(0,0,0,0,0,0,0,1,1,0,0,0,1,1,0,0) \xrightarrow{1r} (0,1,1,0,0,0,1,1,1,0,0,1,0,1,1,0)$	14	8,9,13	2^{-23}
$(0,0,0,0,0,0,0,1,1,0,0,0,1,1,0,1) \xrightarrow{1r} (1,0,0,1,1,1,0,0,0,1,1,0,1,0,0,0)$	14,16,17,18	8,9,13,17,18	$2^{-28.5}$
$(0,0,0,0,0,0,0,1,1,0,0,0,1,1,1,0) \xrightarrow{1r} (1,0,1,0,0,0,1,0,1,0,0,1,0,1,1,0)$	14,18	8,9,13,15,18	2^{-23}
$(0,0,0,0,0,0,0,1,1,0,0,0,1,1,1,1) \xrightarrow{1r} (0,1,0,1,1,1,0,1,0,1,1,0,1,0,0,0)$	14,16,17	8,9,13,15,17	$2^{-28.5}$
$(0,0,0,0,0,0,0,1,1,0,0,1,0,0,0,0) \xrightarrow{1r} (1,0,1,1,0,1,0,1,1,1,1,1,0,1,1,0)$	12,18	8,9,18	$2^{-17.5}$
$(0,0,0,0,0,0,0,1,1,0,0,1,0,0,0,1) \xrightarrow{1r} (0,1,0,0,1,0,1,0,0,0,0,0,1,0,0,0)$	12,16,17	8,9,17	2^{-12}
$(0,0,0,0,0,0,0,1,1,0,0,1,0,0,1,0) \xrightarrow{1r} (0,1,1,1,0,1,0,0,1,1,1,1,0,1,1,0)$	12	8,9,15	$2^{-17.5}$
$(0,0,0,0,0,0,0,1,1,0,0,1,0,0,1,1) \xrightarrow{1r} (1,0,0,0,1,0,1,1,0,0,0,0,1,0,0,0)$	12,16,17,18	8,9,15,17,18	2^{-12}
$(0,0,0,0,0,0,0,1,1,0,0,1,0,1,0,0) \xrightarrow{1r} (0,1,1,0,1,0,0,0,1,0,0,0,1,0,0,1)$	12,14,17	8,9,17	2^{-23}
$(0,0,0,0,0,0,0,1,1,0,0,1,0,1,0,1) \xrightarrow{1r} (1,0,0,1,0,1,1,1,0,1,1,1,0,1,1,1)$	12,14,16,18	8,9,18	$2^{-17.5}$
$(0,0,0,0,0,0,0,1,1,0,0,1,0,1,1,0) \xrightarrow{1r} (1,0,1,0,1,0,0,1,1,0,0,0,1,0,0,1)$	12,14,17,18	8,9,15,17,18	2^{-23}
$(0,0,0,0,0,0,0,1,1,0,0,1,0,1,1,1) \xrightarrow{1r} (0,1,0,1,0,1,1,0,0,1,1,1,0,1,1,1)$	12,14,16	8,9,15	$2^{-17.5}$
$(0,0,0,0,0,0,0,1,1,0,0,1,1,0,0,0) \xrightarrow{1r} (0,1,1,0,0,0,0,1,1,0,1,1,0,1,1,0)$	12	8,9,13	2^{-23}
$(0,0,0,0,0,0,0,1,1,0,0,1,1,0,0,1) \xrightarrow{1r} (1,0,0,1,1,1,1,0,0,1,0,0,1,0,0,0)$	12,16,17,18	8,9,13,17,18	$2^{-17.5}$
$(0,0,0,0,0,0,0,1,1,0,0,1,1,0,1,0) \xrightarrow{1r} (1,0,1,0,0,0,0,0,1,0,1,1,0,1,1,0)$	12,18	8,9,13,15,18	2^{-23}
$(0,0,0,0,0,0,0,1,1,0,0,1,1,0,1,1) \xrightarrow{1r} (0,1,0,1,1,1,1,1,0,1,0,0,1,0,0,0)$	12,16,17	8,9,13,15,17	$2^{-17.5}$
$(0,0,0,0,0,0,0,1,1,0,0,1,1,1,0,0) \xrightarrow{1r} (1,0,1,1,1,1,0,0,1,1,0,0,1,0,0,1)$	12,14,17,18	8,9,13,17,18	$2^{-17.5}$
$(0,0,0,0,0,0,0,1,1,0,0,1,1,1,0,1) \xrightarrow{1r} (0,1,0,0,0,0,1,1,0,0,1,1,0,1,1,1)$	12,14,16	8,9,13	2^{-12}
$(0,0,0,0,0,0,0,1,1,0,0,1,1,1,1,0) \xrightarrow{1r} (0,1,1,1,1,1,0,1,1,1,0,0,1,0,0,1)$	12,14,17	8,9,13,15,17	$2^{-17.5}$
$(0,0,0,0,0,0,0,1,1,0,0,1,1,1,1,1) \xrightarrow{1r} (1,0,0,0,0,0,1,0,0,0,1,1,0,1,1,1)$	12,14,16,18	8,9,13,15,18	2^{-12}

Table 0.14 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	17,18	8,9,11,17,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	16	8,9,11	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	17	8,9,11,15,17	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	16,18	8,9,11,15,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	14	8,9,11	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	14,16,17,18	8,9,11,17,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	14,18	8,9,11,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	14,16,17	8,9,11,15,17	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	17	8,9,11,13,17	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	16,18	8,9,11,13,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	17,18	8,9,11,13,15,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	16	8,9,11,13,15	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	14,18	8,9,11,13,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	14,16,17	8,9,11,13,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	14	8,9,11,13,15	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	14,16,17,18	8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	12	8,9,11	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	12,16,17,18	8,9,11,17,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	12,18	8,9,11,15,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	12,16,17	8,9,11,15,17	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	12,14,17,18	8,9,11,17,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	12,14,16	8,9,11	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	12,14,17	8,9,11,15,17	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	12,14,16,18	8,9,11,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	12,18	8,9,11,13,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	12,16,17	8,9,11,13,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	12	8,9,11,13,15	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	12,16,17,18	8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	12,14,17	8,9,11,13,17	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	12,14,16,18	8,9,11,13,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	12,14,17,18	8,9,11,13,15,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	12,14,16	8,9,11,13,15	2^{-23}

Table 0.15 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	10,18	8,9,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	10,16,17	8,9,17	2^{-1}
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	10	8,9,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	10,16,17,18	8,9,15,17,18	2^{-1}
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	10,14,17	8,9,17	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	10,14,16,18	8,9,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	10,14,17,18	8,9,15,17,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	10,14,16	8,9,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	10	8,9,13	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	10,16,17,18	8,9,13,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	10,18	8,9,13,15,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	10,16,17	8,9,13,15,17	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	10,14,17,18	8,9,13,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	10,14,16	8,9,13	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	10,14,17	8,9,13,15,17	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	10,14,16,18	8,9,13,15,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	10,12,17	8,9,17	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	10,12,16,18	8,9,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	10,12,17,18	8,9,15,17,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	10,12,16	8,9,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	10,12,14,18	8,9,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	10,12,14,16,17	8,9,17	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	10,12,14	8,9,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	10,12,14,16,17,18	8,9,15,17,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	10,12,17,18	8,9,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	10,12,16	8,9,13	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	10,12,17	8,9,13,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	10,12,16,18	8,9,13,15,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	10,12,14	8,9,13	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	10,12,14,16,17,18	8,9,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	10,12,14,18	8,9,13,15,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	10,12,14,16,17	8,9,13,15,17	$2^{-17.5}$

Table 0.16 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,0,0,0,1,1,1,1,0,0,0,0,0) \xrightarrow{1r} (0,1,0,1,1,0,1,1,1,0,1,0,1,1,1,0)$	10	8,9,11	$2^{-28.5}$
$(0,0,0,0,0,0,0,1,1,1,1,0,0,0,0,1) \xrightarrow{1r} (1,0,1,0,0,1,0,0,0,1,0,1,0,0,0,0)$	10,16,17,18	8,9,11,17,18	2^{-12}
$(0,0,0,0,0,0,0,1,1,1,1,0,0,0,1,0) \xrightarrow{1r} (1,0,0,1,1,0,1,0,1,0,1,0,1,1,1,0)$	10,18	8,9,11,15,18	$2^{-28.5}$
$(0,0,0,0,0,0,0,1,1,1,1,0,0,0,1,1) \xrightarrow{1r} (0,1,1,0,0,1,0,1,0,1,0,1,0,0,0,0)$	10,16,17	8,9,11,15,17	2^{-12}
$(0,0,0,0,0,0,0,1,1,1,1,0,0,1,0,0) \xrightarrow{1r} (1,0,0,0,0,1,1,0,1,1,0,1,0,0,0,1)$	10,14,17,18	8,9,11,17,18	2^{-12}
$(0,0,0,0,0,0,0,1,1,1,1,0,0,1,0,1) \xrightarrow{1r} (0,1,1,1,0,0,1,0,0,1,0,1,0,1,1,1)$	10,14,16	8,9,11	$2^{-17.5}$
$(0,0,0,0,0,0,0,1,1,1,1,0,0,1,1,0) \xrightarrow{1r} (0,1,0,0,0,1,1,1,1,1,0,1,0,0,0,1)$	10,14,17	8,9,11,15,17	2^{-12}
$(0,0,0,0,0,0,0,1,1,1,1,0,0,1,1,1) \xrightarrow{1r} (1,0,1,1,1,0,0,0,0,0,1,0,1,1,1,1)$	10,14,16,18	8,9,11,15,18	$2^{-17.5}$
$(0,0,0,0,0,0,0,1,1,1,1,0,1,0,0,0) \xrightarrow{1r} (1,0,0,0,1,1,1,1,1,1,0,1,1,1,0)$	10,18	8,9,11,13,18	2^{-23}
$(0,0,0,0,0,0,0,1,1,1,1,0,1,0,0,1) \xrightarrow{1r} (0,1,1,1,0,0,0,0,0,0,0,1,0,0,0,0)$	10,16,17	8,9,11,13,17	$2^{-6.5}$
$(0,0,0,0,0,0,0,1,1,1,1,0,1,0,1,0) \xrightarrow{1r} (0,1,0,0,1,1,1,0,1,1,1,0,1,1,1,0)$	10	8,9,11,13,15	2^{-23}
$(0,0,0,0,0,0,0,1,1,1,1,0,1,0,1,1) \xrightarrow{1r} (1,0,1,1,0,0,0,1,0,0,0,1,0,0,0,0)$	10,16,17,18	8,9,11,13,15,17,18	$2^{-6.5}$
$(0,0,0,0,0,0,0,1,1,1,1,0,1,1,0,0) \xrightarrow{1r} (0,1,0,1,0,0,1,0,1,0,0,1,0,0,0,1)$	10,14,17	8,9,11,13,17	$2^{-17.5}$
$(0,0,0,0,0,0,0,1,1,1,1,0,1,1,0,1) \xrightarrow{1r} (1,0,1,0,1,1,0,1,0,1,1,0,1,1,1,1)$	10,14,16,18	8,9,11,13,18	2^{-23}
$(0,0,0,0,0,0,0,1,1,1,1,0,1,1,1,0) \xrightarrow{1r} (1,0,0,1,0,0,1,1,1,0,0,1,0,0,0,1)$	10,14,17,18	8,9,11,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,0,0,0,1,1,1,1,0,1,1,1,1) \xrightarrow{1r} (0,1,1,0,1,1,0,0,0,1,1,0,1,1,1,1)$	10,14,16	8,9,11,13,15	2^{-23}
$(0,0,0,0,0,0,0,1,1,1,1,1,0,0,0,0) \xrightarrow{1r} (1,0,0,0,0,1,0,0,1,1,1,1,0,0,0,1)$	10,12,17,18	8,9,11,17,18	2^{-12}
$(0,0,0,0,0,0,0,1,1,1,1,1,0,0,0,1) \xrightarrow{1r} (0,1,1,1,0,1,1,0,0,0,0,1,1,1,1,1)$	10,12,16	8,9,11	$2^{-6.5}$
$(0,0,0,0,0,0,0,1,1,1,1,1,0,0,1,0) \xrightarrow{1r} (0,1,0,0,0,1,0,1,1,1,1,1,0,0,0,1)$	10,12,17	8,9,11,15,17	2^{-12}
$(0,0,0,0,0,0,0,1,1,1,1,1,0,0,1,1) \xrightarrow{1r} (1,0,1,1,1,0,1,0,0,0,0,0,1,1,1,1)$	10,12,16,18	8,9,11,15,18	$2^{-6.5}$
$(0,0,0,0,0,0,0,1,1,1,1,1,0,1,0,0) \xrightarrow{1r} (0,1,0,1,1,0,0,1,1,0,0,0,1,1,1,0)$	10,12,14	8,9,11	$2^{-17.5}$
$(0,0,0,0,0,0,0,1,1,1,1,1,0,1,0,1) \xrightarrow{1r} (1,0,1,0,0,1,1,0,0,1,1,1,0,0,0,0)$	10,12,14,16,17,18	8,9,11,17,18	2^{-12}
$(0,0,0,0,0,0,0,1,1,1,1,1,0,1,1,0) \xrightarrow{1r} (1,0,0,1,1,0,0,0,1,0,0,0,1,1,1,0)$	10,12,14,18	8,9,11,15,18	$2^{-17.5}$
$(0,0,0,0,0,0,0,1,1,1,1,1,0,1,1,1) \xrightarrow{1r} (0,1,1,0,0,1,1,1,0,1,1,1,0,0,0,0)$	10,12,14,16,17	8,9,11,15,17	2^{-12}
$(0,0,0,0,0,0,0,1,1,1,1,1,1,0,0,0) \xrightarrow{1r} (0,1,0,1,0,0,0,0,1,0,1,1,0,0,0,1)$	10,12,17	8,9,11,13,17	$2^{-17.5}$
$(0,0,0,0,0,0,0,1,1,1,1,1,1,0,0,1) \xrightarrow{1r} (1,0,1,0,1,1,1,1,0,1,0,1,0,1,1,1)$	10,12,16,18	8,9,11,13,18	2^{-12}
$(0,0,0,0,0,0,0,1,1,1,1,1,1,0,1,0) \xrightarrow{1r} (1,0,0,1,0,0,0,1,1,0,1,1,0,0,0,1)$	10,12,17,18	8,9,11,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,0,0,0,1,1,1,1,1,1,0,1,1) \xrightarrow{1r} (0,1,1,0,1,1,1,0,0,1,0,0,1,1,1,1)$	10,12,16	8,9,11,13,15	2^{-12}
$(0,0,0,0,0,0,0,1,1,1,1,1,1,1,0,0) \xrightarrow{1r} (1,0,0,0,1,1,0,1,1,1,0,0,1,1,1,0)$	10,12,14,18	8,9,11,13,18	2^{-12}
$(0,0,0,0,0,0,0,1,1,1,1,1,1,1,0,1) \xrightarrow{1r} (0,1,1,1,0,0,1,0,0,0,1,1,0,0,0,0)$	10,12,14,16,17	8,9,11,13,17	$2^{-6.5}$
$(0,0,0,0,0,0,0,1,1,1,1,1,1,1,1,0) \xrightarrow{1r} (0,1,0,0,1,1,0,0,1,1,0,0,1,1,1,0)$	10,12,14	8,9,11,13,15	2^{-12}
$(0,0,0,0,0,0,0,1,1,1,1,1,1,1,1,1) \xrightarrow{1r} (1,0,1,1,0,0,1,1,0,0,1,1,0,0,0,0)$	10,12,14,16,17,18	8,9,11,13,15,17,18	$2^{-6.5}$

Table 0.17 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (1,1,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0)$	7,18	18	2^{-1}
$(0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,1) \xrightarrow{1r} (0,0,1,1,1,1,1,1,1,1,1,1,1,0,1,0)$	7,16,17	17	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,0,0,0,0,0,0,1,0) \xrightarrow{1r} (0,0,0,0,0,0,0,1,0,0,0,0,0,1,0,0)$	7	15	2^{-1}
$(0,0,0,0,0,0,1,0,0,0,0,0,0,0,1,1) \xrightarrow{1r} (1,1,1,1,1,1,1,0,1,1,1,1,1,1,0,1,0)$	7,16,17,18	15,17,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,0,0,0,0,0,1,0,0) \xrightarrow{1r} (0,0,0,1,1,1,0,1,0,1,1,1,1,1,0,1,1)$	7,14,17	17	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,0,0,0,0,0,1,0,1) \xrightarrow{1r} (1,1,1,0,0,0,1,0,1,0,0,0,0,1,0,1)$	7,14,16,18	18	2^{-12}
$(0,0,0,0,0,0,1,0,0,0,0,0,0,1,1,0) \xrightarrow{1r} (1,1,0,1,1,1,0,0,0,1,1,1,1,0,1,1)$	7,14,17,18	15,17,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,0,0,0,0,0,1,1,1) \xrightarrow{1r} (0,0,1,0,0,0,1,1,1,0,0,0,0,1,0,1)$	7,14,16	15	2^{-12}
$(0,0,0,0,0,0,1,0,0,0,0,0,1,0,0,0) \xrightarrow{1r} (0,0,0,1,0,1,0,0,0,1,0,0,0,1,0,0)$	7	13	$2^{-6.5}$
$(0,0,0,0,0,0,1,0,0,0,0,0,1,0,0,1) \xrightarrow{1r} (1,1,1,0,1,0,1,1,1,0,1,1,1,0,1,0)$	7,16,17,18	13,17,18	2^{-23}
$(0,0,0,0,0,0,1,0,0,0,0,0,1,0,1,0) \xrightarrow{1r} (1,1,0,1,0,1,0,1,0,1,0,0,0,1,0,0)$	7,18	13,15,18	$2^{-6.5}$
$(0,0,0,0,0,0,1,0,0,0,0,0,1,0,1,1) \xrightarrow{1r} (0,0,1,0,1,0,1,0,1,0,1,0,1,1,0,1,0)$	7,16,17	13,15,17	2^{-23}
$(0,0,0,0,0,0,1,0,0,0,0,0,1,1,0,0) \xrightarrow{1r} (1,1,0,0,1,0,0,1,0,0,1,1,1,1,0,1,1)$	7,14,17,18	13,17,18	2^{-12}
$(0,0,0,0,0,0,1,0,0,0,0,0,1,1,0,1) \xrightarrow{1r} (0,0,1,1,0,1,1,0,1,1,0,0,0,1,0,1)$	7,14,16	13	$2^{-6.5}$
$(0,0,0,0,0,0,1,0,0,0,0,0,1,1,1,0) \xrightarrow{1r} (0,0,0,0,1,0,0,0,0,0,1,1,1,0,1,1)$	7,14,17	13,15,17	2^{-12}
$(0,0,0,0,0,0,1,0,0,0,0,0,1,1,1,1) \xrightarrow{1r} (1,1,1,1,0,1,1,1,1,1,0,0,0,1,0,1)$	7,14,16,18	13,15,18	$2^{-6.5}$
$(0,0,0,0,0,0,1,0,0,0,0,1,0,0,0,0) \xrightarrow{1r} (0,0,0,1,1,1,1,1,0,1,0,1,1,0,1,1)$	7,12,17	17	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,0,0,0,1,0,0,0,1) \xrightarrow{1r} (1,1,1,0,0,0,0,0,1,0,1,0,0,1,0,1)$	7,12,16,18	18	2^{-23}
$(0,0,0,0,0,0,1,0,0,0,0,1,0,0,1,0) \xrightarrow{1r} (1,1,0,1,1,1,1,0,0,1,0,1,1,0,1,1)$	7,12,17,18	15,17,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,0,0,0,1,0,0,1,1) \xrightarrow{1r} (0,0,1,0,0,0,0,1,1,0,1,0,0,1,0,1)$	7,12,16	15	2^{-23}
$(0,0,0,0,0,0,1,0,0,0,0,1,0,1,0,0) \xrightarrow{1r} (1,1,0,0,0,0,1,0,0,0,1,0,0,1,0,0)$	7,12,14,18	18	2^{-12}
$(0,0,0,0,0,0,1,0,0,0,0,1,0,1,0,1) \xrightarrow{1r} (0,0,1,1,1,1,0,1,1,1,0,1,1,0,1,0)$	7,12,14,16,17	17	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,0,0,0,1,0,1,1,0) \xrightarrow{1r} (0,0,0,0,0,0,1,1,0,0,1,0,0,1,0,0)$	7,12,14	15	2^{-12}
$(0,0,0,0,0,0,1,0,0,0,0,1,0,1,1,1) \xrightarrow{1r} (1,1,1,1,1,1,0,0,1,1,0,1,1,0,1,0)$	7,12,14,16,17,18	15,17,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,0,0,0,1,1,0,0,0) \xrightarrow{1r} (1,1,0,0,1,0,1,1,0,0,0,1,1,0,1,1)$	7,12,17,18	13,17,18	2^{-12}
$(0,0,0,0,0,0,1,0,0,0,0,1,1,0,0,1) \xrightarrow{1r} (0,0,1,1,0,1,0,0,1,1,1,0,0,1,0,1)$	7,12,16	13	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,0,0,0,1,1,0,1,0) \xrightarrow{1r} (0,0,0,0,1,0,1,0,0,0,0,1,1,0,1,1)$	7,12,17	13,15,17	2^{-12}
$(0,0,0,0,0,0,1,0,0,0,0,1,1,0,1,1) \xrightarrow{1r} (1,1,1,1,0,1,0,1,1,1,1,0,0,1,0,1)$	7,12,16,18	13,15,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,0,0,0,1,1,1,0,0) \xrightarrow{1r} (0,0,0,1,0,1,1,0,0,1,1,0,0,1,0,0)$	7,12,14	13	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,0,0,0,1,1,1,0,1) \xrightarrow{1r} (1,1,1,0,1,0,0,1,1,0,0,1,1,0,1,0)$	7,12,14,16,17,18	13,17,18	2^{-23}
$(0,0,0,0,0,0,1,0,0,0,0,1,1,1,1,0) \xrightarrow{1r} (1,1,0,1,0,1,1,1,0,1,1,0,0,1,0,0)$	7,12,14,18	13,15,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,0,0,0,1,1,1,1,1) \xrightarrow{1r} (0,0,1,0,1,0,0,0,1,0,0,1,1,0,1,0)$	7,12,14,16,17	13,15,17	2^{-23}

Table 0.18 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	7	11	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	7,16,17,18	11,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	7,18	11,15,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	7,16,17	11,15,17	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	7,14,17,18	11,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	7,14,16	11	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	7,14,17	11,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	7,14,16,18	11,15,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	7,18	11,13,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	7,16,17	11,13,17	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	7	11,13,15	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	7,16,17,18	11,13,15,17,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	7,14,17	11,13,17	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	7,14,16,18	11,13,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	7,14,17,18	11,13,15,17,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	7,14,16	11,13,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	7,12,17,18	11,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	7,12,16	11	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	7,12,17	11,15,17	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	7,12,16,18	11,15,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	7,12,14	11	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	7,12,14,16,17,18	11,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	7,12,14,18	11,15,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	7,12,14,16,17	11,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	7,12,17	11,13,17	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	7,12,16,18	11,13,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	7,12,17,18	11,13,15,17,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	7,12,16	11,13,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	7,12,14,18	11,13,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	7,12,14,16,17	11,13,17	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	7,12,14	11,13,15	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	7,12,14,16,17,18	11,13,15,17,18	2^{-12}

Table 0.19 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,0,0,1,0,0,1,0,0,0,0,0,0) \xrightarrow{1r} (0,0,1,1,0,1,0,1,0,1,0,1,0,0,1,1)$	7,10,17	17	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,0,1,0,0,0,0,0,1) \xrightarrow{1r} (1,1,0,0,1,0,1,0,1,0,1,0,1,1,0,1)$	7,10,16,18	18	2^{-34}
$(0,0,0,0,0,0,1,0,0,1,0,0,0,0,1,0) \xrightarrow{1r} (1,1,1,1,0,1,0,0,0,1,0,1,0,0,1,1)$	7,10,17,18	15,17,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,0,1,0,0,0,0,1,1) \xrightarrow{1r} (0,0,0,0,1,0,1,1,1,0,1,0,1,1,0,1)$	7,10,16	15	2^{-34}
$(0,0,0,0,0,0,1,0,0,1,0,0,0,1,0,0) \xrightarrow{1r} (1,1,1,0,1,0,0,0,0,0,1,0,1,1,0,0)$	7,10,14,18	18	2^{-23}
$(0,0,0,0,0,0,1,0,0,1,0,0,0,1,0,1) \xrightarrow{1r} (0,0,0,1,0,1,1,1,1,0,1,0,0,1,0,0)$	7,10,14,16,17	17	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,0,1,0,0,0,1,1,0) \xrightarrow{1r} (0,0,1,0,1,0,0,1,0,0,1,0,1,1,0,0)$	7,10,14	15	2^{-23}
$(0,0,0,0,0,0,1,0,0,1,0,0,0,1,1,1) \xrightarrow{1r} (1,1,0,1,0,1,1,0,1,1,0,1,0,0,1,0)$	7,10,14,16,17,18	15,17,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,0,1,0,0,1,0,0,0) \xrightarrow{1r} (1,1,1,0,0,0,0,1,0,0,0,1,0,0,1,1)$	7,10,17,18	13,17,18	2^{-12}
$(0,0,0,0,0,0,1,0,0,1,0,0,1,0,0,1) \xrightarrow{1r} (0,0,0,1,1,1,1,0,1,1,1,0,1,1,0,1)$	7,10,16	13	$2^{-28.5}$
$(0,0,0,0,0,0,1,0,0,1,0,0,1,0,1,0) \xrightarrow{1r} (0,0,1,0,0,0,0,0,0,0,0,0,1,0,0,1)$	7,10,17	13,15,17	2^{-12}
$(0,0,0,0,0,0,1,0,0,1,0,0,1,0,1,1) \xrightarrow{1r} (1,1,0,1,1,1,1,1,1,1,0,1,1,0,1,1)$	7,10,16,18	13,15,18	$2^{-28.5}$
$(0,0,0,0,0,0,1,0,0,1,0,0,1,1,0,0) \xrightarrow{1r} (0,0,1,1,1,1,0,0,0,1,1,0,1,1,0,0)$	7,10,14	13	$2^{-28.5}$
$(0,0,0,0,0,0,1,0,0,1,0,0,1,1,0,1) \xrightarrow{1r} (1,1,0,0,0,0,1,1,1,0,0,1,0,0,1,0)$	7,10,14,16,17,18	13,17,18	2^{-23}
$(0,0,0,0,0,0,1,0,0,1,0,0,1,1,1,0) \xrightarrow{1r} (1,1,1,1,1,1,0,1,0,1,1,0,1,1,0,0)$	7,10,14,18	13,15,18	$2^{-28.5}$
$(0,0,0,0,0,0,1,0,0,1,0,0,1,1,1,1) \xrightarrow{1r} (0,0,0,0,0,0,1,0,1,0,0,1,0,0,1,0)$	7,10,14,16,17	13,15,17	2^{-23}
$(0,0,0,0,0,0,1,0,0,1,0,1,0,0,0,0) \xrightarrow{1r} (1,1,1,0,1,0,1,0,0,0,0,0,1,1,0,0)$	7,10,12,18	18	2^{-12}
$(0,0,0,0,0,0,1,0,0,1,0,1,0,0,0,1) \xrightarrow{1r} (0,0,0,1,0,1,0,1,1,1,1,1,0,0,1,0)$	7,10,12,16,17	17	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,0,1,0,1,0,0,1,0) \xrightarrow{1r} (0,0,1,0,1,0,1,1,0,0,0,0,1,1,0,0)$	7,10,12	15	2^{-12}
$(0,0,0,0,0,0,1,0,0,1,0,1,0,0,1,1) \xrightarrow{1r} (1,1,0,1,0,1,0,0,1,1,1,1,0,0,1,0)$	7,10,12,16,17,18	15,17,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,0,1,0,1,0,1,0,0) \xrightarrow{1r} (0,0,1,1,0,1,1,1,0,1,1,1,0,0,1,1)$	7,10,12,14,17	17	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,0,1,0,1,0,1,0,1) \xrightarrow{1r} (1,1,0,0,1,0,0,0,1,0,0,0,1,1,0,1)$	7,10,12,14,16,18	18	2^{-23}
$(0,0,0,0,0,0,1,0,0,1,0,1,0,1,1,0) \xrightarrow{1r} (1,1,1,1,0,1,1,0,0,1,1,1,0,0,1,1)$	7,10,12,14,17,18	15,17,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,0,1,0,1,0,1,1,1) \xrightarrow{1r} (0,0,0,0,1,0,0,1,1,0,0,0,1,1,0,1)$	7,10,12,14,16	15	2^{-23}
$(0,0,0,0,0,0,1,0,0,1,0,1,0,1,0,0) \xrightarrow{1r} (0,0,1,1,1,1,1,0,0,1,0,0,1,1,0,0)$	7,10,12	13	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,0,1,0,1,1,0,0,1) \xrightarrow{1r} (1,1,0,0,0,0,0,1,1,0,1,1,0,0,1,0)$	7,10,12,16,17,18	13,17,18	2^{-23}
$(0,0,0,0,0,0,1,0,0,1,0,1,1,0,1,0) \xrightarrow{1r} (1,1,1,1,1,1,1,0,1,0,0,1,1,0,0)$	7,10,12,18	13,15,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,0,1,0,1,1,0,1,1) \xrightarrow{1r} (0,0,0,0,0,0,0,0,1,0,1,1,0,0,1,0)$	7,10,12,16,17	13,15,17	2^{-23}
$(0,0,0,0,0,0,1,0,0,1,0,1,1,1,0,0) \xrightarrow{1r} (1,1,1,0,0,0,1,1,0,0,1,1,0,0,1,1)$	7,10,12,14,17,18	13,17,18	2^{-12}
$(0,0,0,0,0,0,1,0,0,1,0,1,1,1,0,1) \xrightarrow{1r} (0,0,0,1,1,1,0,0,1,1,0,0,1,1,0,1)$	7,10,12,14,16	13	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,0,1,0,1,1,1,1,0) \xrightarrow{1r} (0,0,1,0,0,0,1,0,0,0,1,1,0,0,1,1)$	7,10,12,14,17	13,15,17	2^{-12}
$(0,0,0,0,0,0,1,0,0,1,0,1,1,1,1,1) \xrightarrow{1r} (1,1,0,1,1,1,0,1,1,1,0,0,1,1,0,1)$	7,10,12,14,16,18	13,15,18	$2^{-17.5}$

Table 0.20 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	7,10,17,18	11,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	7,10,16	11	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	7,10,17	11,15,17	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	7,10,16,18	11,15,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	7,10,14	11	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	7,10,14,16,17,18	11,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	7,10,14,18	11,15,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	7,10,14,16,17	11,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	7,10,17	11,13,17	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	7,10,16,18	11,13,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	7,10,17,18	11,13,15,17,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	7,10,16	11,13,15	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	7,10,14,18	11,13,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	7,10,14,16,17	11,13,17	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	7,10,14	11,13,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	7,10,14,16,17,18	11,13,15,17,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	7,10,12	11	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	7,10,12,16,17,18	11,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	7,10,12,18	11,15,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	7,10,12,16,17	11,15,17	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	7,10,12,14,17,18	11,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	7,10,12,14,16	11	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	7,10,12,14,17	11,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	7,10,12,14,16,18	11,15,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	7,10,12,18	11,13,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	7,10,12,16,17	11,13,17	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	7,10,12	11,13,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	7,10,12,16,17,18	11,13,15,17,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	7,10,12,14,17	11,13,17	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	7,10,12,14,16,18	11,13,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	7,10,12,14,17,18	11,13,15,17,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	7,10,12,14,16	11,13,15	$2^{-28.5}$

Table 0.21 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	7	9	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	7,16,17,18	9,17,18	2^{-34}
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	7,18	9,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	7,16,17	9,15,17	2^{-34}
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	7,14,17,18	9,17,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	7,14,16	9	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	7,14,17	9,15,17	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	7,14,16,18	9,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	7,18	9,13,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	7,16,17	9,13,17	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	7	9,13,15	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	7,16,17,18	9,13,15,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	7,14,17	9,13,17	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	7,14,16,18	9,13,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	7,14,17,18	9,13,15,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	7,14,16	9,13,15	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	7,12,17,18	9,17,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	7,12,16	9	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	7,12,17	9,15,17	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	7,12,16,18	9,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	7,12,14	9	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	7,12,14,16,17,18	9,17,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	7,12,14,18	9,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	7,12,14,16,17	9,15,17	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	7,12,17	9,13,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	7,12,16,18	9,13,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	7,12,17,18	9,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	7,12,16	9,13,15	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	7,12,14,18	9,13,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	7,12,14,16,17	9,13,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	7,12,14	9,13,15	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	7,12,14,16,17,18	9,13,15,17,18	$2^{-17.5}$

Table 0.22 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	7,18	9,11,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	7,16,17	9,11,17	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	7	9,11,15	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	7,16,17,18	9,11,15,17,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	7,14,17	9,11,17	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	7,14,16,18	9,11,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	7,14,17,18	9,11,15,17,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	7,14,16	9,11,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	7	9,11,13	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	7,16,17,18	9,11,13,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	7,18	9,11,13,15,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	7,16,17	9,11,13,15,17	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	7,14,17,18	9,11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	7,14,16	9,11,13	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	7,14,17	9,11,13,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	7,14,16,18	9,11,13,15,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	7,12,17	9,11,17	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	7,12,16,18	9,11,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	7,12,17,18	9,11,15,17,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	7,12,16	9,11,15	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	7,12,14,18	9,11,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	7,12,14,16,17	9,11,17	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	7,12,14	9,11,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	7,12,14,16,17,18	9,11,15,17,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	7,12,17,18	9,11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	7,12,16	9,11,13	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	7,12,17	9,11,13,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	7,12,16,18	9,11,13,15,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	7,12,14	9,11,13	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	7,12,14,16,17,18	9,11,13,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	7,12,14,18	9,11,13,15,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	7,12,14,16,17	9,11,13,15,17	$2^{-28.5}$

Table 0.23 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,0,0,1,0,1,1,0,0,0,0,0,0) \xrightarrow{1r} (1,0,1,0,0,0,0,0,0,0,0,0,0,1,1,1)$	7,10,17,18	9,17,18	2^{-1}
$(0,0,0,0,0,0,1,0,1,1,0,0,0,0,0,1) \xrightarrow{1r} (0,1,0,1,1,1,1,1,1,1,1,1,1,0,0,1)$	7,10,16	9	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,1,1,0,0,0,0,1,0) \xrightarrow{1r} (0,1,1,0,0,0,0,1,0,0,0,0,0,1,1,1)$	7,10,17	9,15,17	2^{-1}
$(0,0,0,0,0,0,1,0,1,1,0,0,0,0,1,1) \xrightarrow{1r} (1,0,0,1,1,1,1,0,1,1,1,1,1,1,0,0,1)$	7,10,16,18	9,15,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,1,1,0,0,0,1,0,0) \xrightarrow{1r} (0,1,1,1,1,1,0,1,0,1,1,1,1,1,0,0,0)$	7,10,14	9	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,1,1,0,0,0,1,0,1) \xrightarrow{1r} (1,0,0,0,0,0,1,0,1,0,0,0,0,1,1,0)$	7,10,14,16,17,18	9,17,18	2^{-12}
$(0,0,0,0,0,0,1,0,1,1,0,0,0,1,1,0) \xrightarrow{1r} (1,0,1,1,1,1,0,0,0,1,1,1,1,1,0,0,0)$	7,10,14,18	9,15,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,1,1,0,0,0,1,1,1) \xrightarrow{1r} (0,1,0,0,0,0,1,1,1,0,0,0,0,1,1,0)$	7,10,14,16,17	9,15,17	2^{-12}
$(0,0,0,0,0,0,1,0,1,1,0,0,1,0,0,0) \xrightarrow{1r} (0,1,1,1,0,1,0,0,0,1,0,0,0,1,1,1)$	7,10,17	9,13,17	$2^{-6.5}$
$(0,0,0,0,0,0,1,0,1,1,0,0,1,0,0,1) \xrightarrow{1r} (1,0,0,0,1,0,1,1,1,0,1,1,1,0,0,1)$	7,10,16,18	9,13,18	2^{-23}
$(0,0,0,0,0,0,1,0,1,1,0,0,1,0,1,0) \xrightarrow{1r} (1,0,1,1,0,1,0,1,0,1,0,0,0,1,1,1)$	7,10,17,18	9,13,15,17,18	$2^{-6.5}$
$(0,0,0,0,0,0,1,0,1,1,0,0,1,0,1,1) \xrightarrow{1r} (0,1,0,0,1,0,1,0,1,0,1,0,1,1,1,0,0,1)$	7,10,16	9,13,15	2^{-23}
$(0,0,0,0,0,0,1,0,1,1,0,0,1,1,0,0) \xrightarrow{1r} (1,0,1,0,1,0,0,1,0,0,1,1,1,1,0,0,0)$	7,10,14,18	9,13,18	2^{-12}
$(0,0,0,0,0,0,1,0,1,1,0,0,1,1,0,1) \xrightarrow{1r} (0,1,0,1,0,1,1,0,1,1,0,0,0,1,1,0)$	7,10,14,16,17	9,13,17	$2^{-6.5}$
$(0,0,0,0,0,0,1,0,1,1,0,0,1,1,1,0) \xrightarrow{1r} (0,1,1,0,1,0,0,0,0,0,1,1,1,0,0,0)$	7,10,14	9,13,15	2^{-12}
$(0,0,0,0,0,0,1,0,1,1,0,0,1,1,1,1) \xrightarrow{1r} (1,0,0,1,0,1,1,1,1,1,0,0,0,1,1,0)$	7,10,14,16,17,18	9,13,15,17,18	$2^{-6.5}$
$(0,0,0,0,0,0,1,0,1,1,0,1,0,0,0,0) \xrightarrow{1r} (0,1,1,1,1,1,1,1,0,1,0,1,1,0,0,0)$	7,10,12	9	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,1,1,0,1,0,0,0,1) \xrightarrow{1r} (1,0,0,0,0,0,0,0,1,0,1,0,0,1,1,0)$	7,10,12,16,17,18	9,17,18	2^{-23}
$(0,0,0,0,0,0,1,0,1,1,0,1,0,0,1,0) \xrightarrow{1r} (1,0,1,1,1,1,1,0,0,1,0,1,1,0,0,0)$	7,10,12,18	9,15,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,1,1,0,1,0,0,1,1) \xrightarrow{1r} (0,1,0,0,0,0,0,1,1,0,1,0,0,1,1,0)$	7,10,12,16,17	9,15,17	2^{-23}
$(0,0,0,0,0,0,1,0,1,1,0,1,0,1,0,0) \xrightarrow{1r} (1,0,1,0,0,0,1,0,0,0,1,0,0,1,1,1)$	7,10,12,14,17,18	9,17,18	2^{-12}
$(0,0,0,0,0,0,1,0,1,1,0,1,0,1,0,1) \xrightarrow{1r} (0,1,0,1,1,1,0,1,1,1,0,1,1,0,0,1)$	7,10,12,14,16	9	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,1,1,0,1,0,1,1,1) \xrightarrow{1r} (0,1,1,0,0,0,1,1,0,0,1,0,0,1,1,1)$	7,10,12,14,17	9,15,17	2^{-12}
$(0,0,0,0,0,0,1,0,1,1,0,1,0,1,1,1) \xrightarrow{1r} (1,0,0,1,1,1,0,0,1,1,0,1,1,0,0,1)$	7,10,12,14,16,18	9,15,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,1,1,0,1,1,0,0,0) \xrightarrow{1r} (1,0,1,0,1,0,1,1,0,0,0,1,1,0,0,0)$	7,10,12,18	9,13,18	2^{-12}
$(0,0,0,0,0,0,1,0,1,1,0,1,1,0,0,1) \xrightarrow{1r} (0,1,0,1,0,1,0,0,1,1,1,0,0,1,1,0)$	7,10,12,16,17	9,13,17	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,1,1,0,1,1,0,1,0) \xrightarrow{1r} (0,1,1,0,1,0,1,0,0,0,0,1,1,0,0,0)$	7,10,12	9,13,15	2^{-12}
$(0,0,0,0,0,0,1,0,1,1,0,1,1,0,1,1) \xrightarrow{1r} (1,0,0,1,0,1,0,1,1,1,1,0,0,1,1,0)$	7,10,12,16,17,18	9,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,1,1,0,1,1,1,0,0) \xrightarrow{1r} (0,1,1,1,0,1,1,0,0,1,1,0,0,1,1,1)$	7,10,12,14,17	9,13,17	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,1,1,0,1,1,1,0,1) \xrightarrow{1r} (1,0,0,0,1,0,0,1,1,0,0,1,1,0,0,1)$	7,10,12,14,16,18	9,13,18	2^{-23}
$(0,0,0,0,0,0,1,0,1,1,0,1,1,1,1,0) \xrightarrow{1r} (1,0,1,1,0,1,1,1,0,1,1,0,0,1,1,1)$	7,10,12,14,17,18	9,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,1,1,0,1,1,1,1,1) \xrightarrow{1r} (0,1,0,0,1,0,0,0,1,0,0,1,1,0,0,1)$	7,10,12,14,16	9,13,15	2^{-23}

Table 0.24 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,0,0,1,0,1,1,1,0,0,0,0,0) \xrightarrow{1r} (0,1,1,0,0,1,0,0,0,1,0,1,0,1,1,1)$	7,10,17	9,11,17	2^{-12}
$(0,0,0,0,0,0,1,0,1,1,1,0,0,0,0,1) \xrightarrow{1r} (1,0,0,1,1,0,1,1,1,0,1,0,1,0,0,1)$	7,10,16,18	9,11,18	$2^{-28.5}$
$(0,0,0,0,0,0,1,0,1,1,1,0,0,0,1,0) \xrightarrow{1r} (1,0,1,0,0,1,0,1,0,1,0,1,0,1,1,1)$	7,10,17,18	9,11,15,17,18	2^{-12}
$(0,0,0,0,0,0,1,0,1,1,1,0,0,0,1,1) \xrightarrow{1r} (0,1,0,1,1,0,1,0,1,0,1,0,1,0,0,1)$	7,10,16	9,11,15	$2^{-28.5}$
$(0,0,0,0,0,0,1,0,1,1,1,0,0,1,0,0) \xrightarrow{1r} (1,0,1,1,1,0,0,1,0,0,1,0,1,0,0,0)$	7,10,14,18	9,11,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,1,1,1,0,0,1,0,1) \xrightarrow{1r} (0,1,0,0,0,1,1,0,1,1,0,1,0,1,1,0)$	7,10,14,16,17	9,11,17	2^{-12}
$(0,0,0,0,0,0,1,0,1,1,1,0,0,1,1,0) \xrightarrow{1r} (0,1,1,1,1,0,0,0,0,0,1,0,1,0,0,0)$	7,10,14	9,11,15	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,1,1,1,0,0,1,1,1) \xrightarrow{1r} (1,0,0,0,0,1,1,1,1,1,0,1,0,1,1,0)$	7,10,14,16,17,18	9,11,15,17,18	2^{-12}
$(0,0,0,0,0,0,1,0,1,1,1,0,1,0,0,0) \xrightarrow{1r} (1,0,1,1,0,0,0,0,0,0,0,0,1,0,1,1)$	7,10,17,18	9,11,13,17,18	$2^{-6.5}$
$(0,0,0,0,0,0,1,0,1,1,1,0,1,0,0,1) \xrightarrow{1r} (0,1,0,0,1,1,1,1,1,1,0,1,0,0,0,1)$	7,10,16	9,11,13	2^{-23}
$(0,0,0,0,0,0,1,0,1,1,1,0,1,0,1,0) \xrightarrow{1r} (0,1,1,1,0,0,0,1,0,0,0,1,0,1,1,1)$	7,10,17	9,11,13,15,17	$2^{-6.5}$
$(0,0,0,0,0,0,1,0,1,1,1,0,1,0,1,1) \xrightarrow{1r} (1,0,0,0,1,1,1,0,1,1,1,0,1,0,0,1)$	7,10,16,18	9,11,13,15,18	2^{-23}
$(0,0,0,0,0,0,1,0,1,1,1,0,1,1,0,0) \xrightarrow{1r} (0,1,1,0,1,1,0,1,0,1,1,0,1,0,0,0)$	7,10,14	9,11,13	2^{-23}
$(0,0,0,0,0,0,1,0,1,1,1,0,1,1,0,1) \xrightarrow{1r} (1,0,0,1,0,0,1,0,1,0,0,1,0,1,1,0)$	7,10,14,16,17,18	9,11,13,17,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,1,1,1,0,1,1,1,0) \xrightarrow{1r} (1,0,1,0,1,1,0,0,0,1,1,0,1,0,0,0)$	7,10,14,18	9,11,13,15,18	2^{-23}
$(0,0,0,0,0,0,1,0,1,1,1,0,1,1,1,1) \xrightarrow{1r} (0,1,0,1,0,0,1,1,1,0,0,1,0,1,1,0)$	7,10,14,16,17	9,11,13,15,17	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,1,1,1,1,0,0,0,0) \xrightarrow{1r} (1,0,1,1,1,0,1,1,0,0,0,0,1,0,0,0)$	7,10,12,18	9,11,18	$2^{-6.5}$
$(0,0,0,0,0,0,1,0,1,1,1,1,0,0,0,1) \xrightarrow{1r} (0,1,0,0,0,1,0,0,1,1,1,1,0,1,1,0)$	7,10,12,16,17	9,11,17	2^{-12}
$(0,0,0,0,0,0,1,0,1,1,1,1,0,0,1,0) \xrightarrow{1r} (0,1,1,1,1,0,1,0,0,0,0,0,1,0,0,0)$	7,10,12	9,11,15	$2^{-6.5}$
$(0,0,0,0,0,0,1,0,1,1,1,1,0,0,1,1) \xrightarrow{1r} (1,0,0,0,0,1,0,1,1,1,1,1,0,1,1,0)$	7,10,12,16,17,18	9,11,15,17,18	2^{-12}
$(0,0,0,0,0,0,1,0,1,1,1,1,0,1,0,0) \xrightarrow{1r} (0,1,1,0,0,1,1,0,0,1,1,1,0,1,1,1)$	7,10,12,14,17	9,11,17	2^{-12}
$(0,0,0,0,0,0,1,0,1,1,1,1,0,1,0,1) \xrightarrow{1r} (1,0,0,1,1,0,0,1,1,0,0,0,1,0,0,1)$	7,10,12,14,16,18	9,11,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,1,1,1,1,0,1,1,1) \xrightarrow{1r} (1,0,1,0,0,1,1,1,0,1,1,1,0,1,1,1)$	7,10,12,14,17,18	9,11,15,17,18	2^{-12}
$(0,0,0,0,0,0,1,0,1,1,1,1,1,0,0,1) \xrightarrow{1r} (0,1,0,1,1,0,0,0,1,0,0,0,1,0,0,1)$	7,10,12,14,16	9,11,15	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,1,1,1,1,1,0,0,0) \xrightarrow{1r} (0,1,1,0,1,1,1,1,0,1,0,0,1,0,0,0)$	7,10,12	9,11,13	2^{-12}
$(0,0,0,0,0,0,1,0,1,1,1,1,1,0,0,1) \xrightarrow{1r} (1,0,0,1,0,0,0,0,1,0,1,1,0,1,1,0)$	7,10,12,16,17,18	9,11,13,17,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,1,1,1,1,1,0,1,0) \xrightarrow{1r} (1,0,1,0,1,1,1,0,0,1,0,0,1,0,0,0)$	7,10,12,18	9,11,13,15,18	2^{-12}
$(0,0,0,0,0,0,1,0,1,1,1,1,1,0,1,1) \xrightarrow{1r} (0,1,0,1,0,0,0,1,1,0,1,1,0,1,1,0)$	7,10,12,16,17	9,11,13,15,17	$2^{-17.5}$
$(0,0,0,0,0,0,1,0,1,1,1,1,1,1,0,0) \xrightarrow{1r} (1,0,1,1,0,0,1,0,0,0,1,1,0,1,1,1)$	7,10,12,14,17,18	9,11,13,17,18	$2^{-6.5}$
$(0,0,0,0,0,0,1,0,1,1,1,1,1,1,0,1) \xrightarrow{1r} (0,1,0,0,1,1,0,1,1,1,0,0,1,0,0,1)$	7,10,12,14,16	9,11,13	2^{-12}
$(0,0,0,0,0,0,1,0,1,1,1,1,1,1,1,0) \xrightarrow{1r} (0,1,1,1,0,0,1,1,0,0,1,1,0,1,1,1)$	7,10,12,14,17	9,11,13,15,17	$2^{-6.5}$
$(0,0,0,0,0,0,1,0,1,1,1,1,1,1,1,1) \xrightarrow{1r} (1,0,0,0,1,1,0,0,1,1,0,0,1,0,0,1)$	7,10,12,14,16,18	9,11,13,15,18	2^{-12}

Table 0.25 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	7,17	8,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	7,16,18	8,18	2^{-1}
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	7,17,18	8,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	7,16	8,15	2^{-1}
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	7,14,18	8,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	7,14,16,17	8,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	7,14	8,15	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	7,14,16,17,18	8,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	7,17,18	8,13,17,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	7,16	8,13	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	7,17	8,13,15,17	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	7,16,18	8,13,15,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	7,14	8,13	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	7,14,16,17,18	8,13,17,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	7,14,18	8,13,15,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	7,14,16,17	8,13,15,17	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	7,12,18	8,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	7,12,16,17	8,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	7,12	8,15	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	7,12,16,17,18	8,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	7,12,14,17	8,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	7,12,14,16,18	8,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	7,12,14,17,18	8,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	7,12,14,16	8,15	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	7,12	8,13	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	7,12,16,17,18	8,13,17,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	7,12,18	8,13,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	7,12,16,17	8,13,15,17	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	7,12,14,17,18	8,13,17,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	7,12,14,16	8,13	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	7,12,14,17	8,13,15,17	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	7,12,14,16,18	8,13,15,18	$2^{-17.5}$

Table 0.26 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,0,0,1,1,0,0,1,0,0,0,0,0) \xrightarrow{1r} (1,1,1,1,1,0,1,1,1,0,1,0,1,0,0,1)$	7,17,18	8,11,17,18	$2^{-28.5}$
$(0,0,0,0,0,0,1,1,0,0,1,0,0,0,0,1) \xrightarrow{1r} (0,0,0,0,0,1,0,0,0,1,0,1,0,1,1,1)$	7,16	8,11	2^{-12}
$(0,0,0,0,0,0,1,1,0,0,1,0,0,0,1,0) \xrightarrow{1r} (0,0,1,1,1,0,1,0,1,0,1,0,1,0,0,1)$	7,17	8,11,15,17	$2^{-28.5}$
$(0,0,0,0,0,0,1,1,0,0,1,0,0,0,1,1) \xrightarrow{1r} (1,1,0,0,0,1,0,1,0,1,0,1,0,1,1,1)$	7,16,18	8,11,15,18	2^{-12}
$(0,0,0,0,0,0,1,1,0,0,1,0,0,1,0,0) \xrightarrow{1r} (0,0,1,0,0,1,1,0,1,1,0,1,0,1,1,0)$	7,14	8,11	2^{-12}
$(0,0,0,0,0,0,1,1,0,0,1,0,0,1,0,1) \xrightarrow{1r} (1,1,0,1,1,0,0,1,0,0,1,0,1,0,0,0)$	7,14,16,17,18	8,11,17,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,0,0,1,0,0,1,1,0) \xrightarrow{1r} (1,1,1,0,0,1,1,1,1,1,0,1,0,1,1,0)$	7,14,18	8,11,15,18	2^{-12}
$(0,0,0,0,0,0,1,1,0,0,1,0,0,1,1,1) \xrightarrow{1r} (0,0,0,1,1,0,0,0,0,0,1,0,1,0,0,0)$	7,14,16,17	8,11,15,17	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,0,0,1,0,1,0,0,0) \xrightarrow{1r} (0,0,1,0,1,1,1,1,1,1,0,1,0,0,0,1)$	7,17	8,11,13,17	2^{-23}
$(0,0,0,0,0,0,1,1,0,0,1,0,1,0,0,1) \xrightarrow{1r} (1,1,0,1,0,0,0,0,0,0,0,1,0,1,1,1)$	7,16,18	8,11,13,18	$2^{-6.5}$
$(0,0,0,0,0,0,1,1,0,0,1,0,1,0,1,0) \xrightarrow{1r} (1,1,1,0,1,1,1,0,1,1,1,0,1,0,0,1)$	7,17,18	8,11,13,15,17,18	2^{-23}
$(0,0,0,0,0,0,1,1,0,0,1,0,1,0,1,1) \xrightarrow{1r} (0,0,0,1,0,0,0,1,0,0,0,1,0,1,1,1)$	7,16	8,11,13,15	$2^{-6.5}$
$(0,0,0,0,0,0,1,1,0,0,1,0,1,1,0,0) \xrightarrow{1r} (1,1,1,1,0,0,1,0,1,0,0,1,0,1,1,0)$	7,14,18	8,11,13,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,0,0,1,0,1,1,0,1) \xrightarrow{1r} (0,0,0,0,1,1,0,1,0,1,1,0,1,0,0,0)$	7,14,16,17	8,11,13,17	2^{-23}
$(0,0,0,0,0,0,1,1,0,0,1,0,1,1,1,0) \xrightarrow{1r} (0,0,1,1,0,0,1,1,1,0,0,1,0,1,1,0)$	7,14	8,11,13,15	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,0,0,1,0,1,1,1,1) \xrightarrow{1r} (1,1,0,0,1,1,0,0,0,1,1,0,1,0,0,0)$	7,14,16,17,18	8,11,13,15,17,18	2^{-23}
$(0,0,0,0,0,0,1,1,0,0,1,1,0,0,0,0) \xrightarrow{1r} (0,0,1,0,0,1,0,0,1,1,1,1,0,1,1,0)$	7,12	8,11	2^{-12}
$(0,0,0,0,0,0,1,1,0,0,1,1,0,0,0,1) \xrightarrow{1r} (1,1,0,1,1,0,1,1,0,0,0,0,1,0,0,0)$	7,12,16,17,18	8,11,17,18	$2^{-6.5}$
$(0,0,0,0,0,0,1,1,0,0,1,1,0,0,1,0) \xrightarrow{1r} (1,1,1,0,0,1,0,1,1,1,1,1,0,1,1,0)$	7,12,18	8,11,15,18	2^{-12}
$(0,0,0,0,0,0,1,1,0,0,1,1,0,0,1,1) \xrightarrow{1r} (0,0,0,1,1,0,1,0,0,0,0,0,1,0,0,0)$	7,12,16,17	8,11,15,17	$2^{-6.5}$
$(0,0,0,0,0,0,1,1,0,0,1,1,0,0,1,1) \xrightarrow{1r} (1,1,1,1,0,0,1,1,0,0,0,1,0,0,0,1)$	7,12,14,17,18	8,11,17,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,0,0,1,1,0,0,1,0) \xrightarrow{1r} (0,0,0,0,0,1,1,0,0,1,1,1,0,1,1,1)$	7,12,14,16	8,11	2^{-12}
$(0,0,0,0,0,0,1,1,0,0,1,1,0,0,1,1) \xrightarrow{1r} (0,0,1,1,1,0,0,0,1,0,0,0,1,0,0,1)$	7,12,14,17	8,11,15,17	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,0,0,1,1,0,0,1,1) \xrightarrow{1r} (1,1,0,0,0,1,1,1,0,1,1,1,0,1,1,1)$	7,12,14,16,18	8,11,15,18	2^{-12}
$(0,0,0,0,0,0,1,1,0,0,1,1,1,0,0,0) \xrightarrow{1r} (1,1,1,1,0,0,0,0,1,0,1,1,0,1,1,0)$	7,12,18	8,11,13,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,0,0,1,1,1,0,0,1) \xrightarrow{1r} (0,0,0,0,1,1,1,1,0,1,0,0,1,0,0,0)$	7,12,16,17	8,11,13,17	2^{-12}
$(0,0,0,0,0,0,1,1,0,0,1,1,1,0,1,0) \xrightarrow{1r} (0,0,1,1,0,0,0,1,1,0,1,1,0,1,1,0)$	7,12	8,11,13,15	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,0,0,1,1,1,0,1,1) \xrightarrow{1r} (1,1,0,0,1,1,1,0,0,1,0,0,1,0,0,0)$	7,12,16,17,18	8,11,13,15,17,18	2^{-12}
$(0,0,0,0,0,0,1,1,0,0,1,1,1,1,0,0) \xrightarrow{1r} (0,0,1,0,1,1,0,1,1,1,1,0,0,1,0,0,1)$	7,12,14,17	8,11,13,17	2^{-12}
$(0,0,0,0,0,0,1,1,0,0,1,1,1,1,0,1) \xrightarrow{1r} (1,1,0,1,0,0,1,0,0,0,0,1,1,0,1,1,1)$	7,12,14,16,18	8,11,13,18	$2^{-6.5}$
$(0,0,0,0,0,0,1,1,0,0,1,1,1,1,1,0) \xrightarrow{1r} (1,1,1,0,1,1,0,0,1,1,0,0,1,1,0,0,1)$	7,12,14,17,18	8,11,13,15,17,18	2^{-12}
$(0,0,0,0,0,0,1,1,0,0,1,1,1,1,1,1) \xrightarrow{1r} (0,0,0,1,0,0,1,1,0,0,1,1,0,1,1,1)$	7,12,14,16	8,11,13,15	$2^{-6.5}$

Table 0.27 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,0,0,1,1,0,1,0,0,0,0,0,0) \xrightarrow{1r} (1,1,0,0,1,0,1,0,1,0,1,0,1,1,1,0)$	7,10,18	8,18	2^{-34}
$(0,0,0,0,0,0,1,1,0,1,0,0,0,0,0,1) \xrightarrow{1r} (0,0,1,1,0,1,0,1,0,1,0,1,0,0,0,0)$	7,10,16,17	8,17	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,0,1,0,0,0,0,1,0) \xrightarrow{1r} (0,0,0,0,1,0,1,1,1,0,1,0,1,1,1,0)$	7,10	8,15	2^{-34}
$(0,0,0,0,0,0,1,1,0,1,0,0,0,0,1,1) \xrightarrow{1r} (1,1,1,1,0,1,0,0,0,1,0,1,0,0,0,0)$	7,10,16,17,18	8,15,17,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,0,1,0,0,0,1,0,0) \xrightarrow{1r} (0,0,0,1,0,1,1,1,1,1,0,1,0,0,0,1)$	7,10,14,17	8,17	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,0,1,0,0,0,1,0,1) \xrightarrow{1r} (1,1,1,0,1,0,0,0,0,0,1,0,1,1,1,1)$	7,10,14,16,18	8,18	2^{-23}
$(0,0,0,0,0,0,1,1,0,1,0,0,0,1,1,0) \xrightarrow{1r} (1,1,0,1,0,1,1,0,1,1,0,1,0,0,0,1)$	7,10,14,17,18	8,15,17,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,0,1,0,0,0,1,1,1) \xrightarrow{1r} (0,0,1,0,1,0,0,1,0,0,1,0,1,1,1,1)$	7,10,14,16	8,15	2^{-23}
$(0,0,0,0,0,0,1,1,0,1,0,0,1,0,0,0) \xrightarrow{1r} (0,0,0,1,1,1,1,0,1,1,1,0,1,1,1,0)$	7,10	8,13	$2^{-28.5}$
$(0,0,0,0,0,0,1,1,0,1,0,0,1,0,0,1) \xrightarrow{1r} (1,1,1,0,0,0,0,1,0,0,0,1,0,0,0,0)$	7,10,16,17,18	8,13,17,18	2^{-12}
$(0,0,0,0,0,0,1,1,0,1,0,0,1,0,1,0) \xrightarrow{1r} (1,1,0,1,1,1,1,1,1,1,0,1,1,1,0)$	7,10,18	8,13,15,18	$2^{-28.5}$
$(0,0,0,0,0,0,1,1,0,1,0,0,1,0,1,1) \xrightarrow{1r} (0,0,1,0,0,0,0,0,0,0,0,1,0,0,0,0)$	7,10,16,17	8,13,15,17	2^{-12}
$(0,0,0,0,0,0,1,1,0,1,0,0,1,1,0,0) \xrightarrow{1r} (1,1,0,0,0,0,1,1,1,0,0,1,0,0,0,1)$	7,10,14,17,18	8,13,17,18	2^{-23}
$(0,0,0,0,0,0,1,1,0,1,0,0,1,1,0,1) \xrightarrow{1r} (0,0,1,1,1,1,0,0,0,1,1,0,1,1,1,1)$	7,10,14,16	8,13	$2^{-28.5}$
$(0,0,0,0,0,0,1,1,0,1,0,0,1,1,1,0) \xrightarrow{1r} (0,0,0,0,0,0,1,0,1,0,0,1,0,0,0,1)$	7,10,14,17	8,13,15,17	2^{-23}
$(0,0,0,0,0,0,1,1,0,1,0,0,1,1,1,1) \xrightarrow{1r} (1,1,1,1,1,1,0,1,0,1,1,0,1,1,1,1)$	7,10,14,16,18	8,13,15,18	$2^{-28.5}$
$(0,0,0,0,0,0,1,1,0,1,0,1,0,0,0,0) \xrightarrow{1r} (0,0,0,1,0,1,0,1,1,1,1,1,0,0,0,1)$	7,10,12,17	8,17	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,0,1,0,1,0,0,0,1) \xrightarrow{1r} (1,1,1,0,1,0,1,0,0,0,0,0,1,1,1,1)$	7,10,12,16,18	8,18	2^{-12}
$(0,0,0,0,0,0,1,1,0,1,0,1,0,0,1,0) \xrightarrow{1r} (1,1,0,1,0,1,0,0,1,1,1,1,0,0,0,1)$	7,10,12,17,18	8,15,17,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,0,1,0,1,0,0,1,1) \xrightarrow{1r} (0,0,1,0,1,0,1,1,0,0,0,0,1,1,1,1)$	7,10,12,16	8,15	2^{-12}
$(0,0,0,0,0,0,1,1,0,1,0,1,0,1,0,0) \xrightarrow{1r} (1,1,0,0,1,0,0,0,1,0,0,0,1,1,1,0)$	7,10,12,14,18	8,18	2^{-23}
$(0,0,0,0,0,0,1,1,0,1,0,1,0,1,0,1) \xrightarrow{1r} (0,0,1,1,0,1,1,1,0,1,1,1,0,0,0,0)$	7,10,12,14,16,17	8,17	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,0,1,0,1,0,1,1,0) \xrightarrow{1r} (0,0,0,0,1,0,0,1,1,0,0,0,1,1,1,0)$	7,10,12,14	8,15	2^{-23}
$(0,0,0,0,0,0,1,1,0,1,0,1,0,1,1,1) \xrightarrow{1r} (1,1,1,1,0,1,1,0,0,1,1,1,0,0,0,0)$	7,10,12,14,16,17,18	8,15,17,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,0,1,0,1,1,0,0,0) \xrightarrow{1r} (1,1,0,0,0,0,0,1,1,0,1,1,0,0,0,1)$	7,10,12,17,18	8,13,17,18	2^{-23}
$(0,0,0,0,0,0,1,1,0,1,0,1,1,0,0,1) \xrightarrow{1r} (0,0,1,1,1,1,1,0,0,1,0,0,1,1,1,1)$	7,10,12,16	8,13	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,0,1,0,1,1,0,1,0) \xrightarrow{1r} (0,0,0,0,0,0,0,0,1,0,1,1,0,0,0,1)$	7,10,12,17	8,13,15,17	2^{-23}
$(0,0,0,0,0,0,1,1,0,1,0,1,1,0,1,1) \xrightarrow{1r} (1,1,1,1,1,1,1,1,0,1,0,0,1,1,1,1)$	7,10,12,16,18	8,13,15,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,0,1,0,1,1,1,0,0) \xrightarrow{1r} (0,0,0,1,1,1,0,0,1,1,0,0,1,1,1,0)$	7,10,12,14	8,13	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,0,1,0,1,1,1,0,1) \xrightarrow{1r} (1,1,1,0,0,0,1,1,0,0,1,1,0,0,0,0)$	7,10,12,14,16,17,18	8,13,17,18	2^{-12}
$(0,0,0,0,0,0,1,1,0,1,0,1,1,1,1,0) \xrightarrow{1r} (1,1,0,1,1,1,0,1,1,1,0,0,1,1,1,0)$	7,10,12,14,18	8,13,15,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,0,1,0,1,1,1,1,1) \xrightarrow{1r} (0,0,1,0,0,0,1,0,0,0,1,1,0,0,0,0)$	7,10,12,14,16,17	8,13,15,17	2^{-12}

Table 0.28 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	7,10	8,11	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	7,10,16,17,18	8,11,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	7,10,18	8,11,15,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	7,10,16,17	8,11,15,17	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	7,10,14,17,18	8,11,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	7,10,14,16	8,11	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	7,10,14,17	8,11,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	7,10,14,16,18	8,11,15,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	7,10,18	8,11,13,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	7,10,16,17	8,11,13,17	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	7,10	8,11,13,15	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	7,10,16,17,18	8,11,13,15,17,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	7,10,14,17	8,11,13,17	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	7,10,14,16,18	8,11,13,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	7,10,14,17,18	8,11,13,15,17,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	7,10,14,16	8,11,13,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	7,10,12,17,18	8,11,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	7,10,12,16	8,11	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	7,10,12,17	8,11,15,17	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	7,10,12,16,18	8,11,15,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	7,10,12,14	8,11	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	7,10,12,14,16,17,18	8,11,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	7,10,12,14,18	8,11,15,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	7,10,12,14,16,17	8,11,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	7,10,12,17	8,11,13,17	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	7,10,12,16,18	8,11,13,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	7,10,12,17,18	8,11,13,15,17,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	7,10,12,16	8,11,13,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	7,10,12,14,18	8,11,13,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	7,10,12,14,16,17	8,11,13,17	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	7,10,12,14	8,11,13,15	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	7,10,12,14,16,17,18	8,11,13,15,17,18	2^{-23}

Table 0.29 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,0,0,1,1,1,0,0,0,0,0,0,0) \xrightarrow{1r} (1,0,1,0,1,0,1,0,1,0,1,0,1,1,0,1)$	7,17,18	8,9,17,18	2^{-34}
$(0,0,0,0,0,0,1,1,1,0,0,0,0,0,0,1) \xrightarrow{1r} (0,1,0,1,0,1,0,1,0,1,0,1,0,0,1,1)$	7,16	8,9	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,1,0,0,0,0,0,1,0) \xrightarrow{1r} (0,1,1,0,1,0,1,1,1,0,1,0,1,1,0,1)$	7,17	8,9,15,17	2^{-34}
$(0,0,0,0,0,0,1,1,1,0,0,0,0,0,1,1) \xrightarrow{1r} (1,0,0,1,0,1,0,0,0,1,0,1,0,0,1,1)$	7,16,18	8,9,15,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,1,0,0,0,0,1,0,0) \xrightarrow{1r} (0,1,1,1,0,1,1,1,1,1,0,1,0,0,1,0)$	7,14	8,9	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,1,0,0,0,0,1,0,1) \xrightarrow{1r} (1,0,0,0,1,0,0,0,0,0,1,0,1,1,0,0)$	7,14,16,17,18	8,9,17,18	2^{-23}
$(0,0,0,0,0,0,1,1,1,0,0,0,0,1,1,0) \xrightarrow{1r} (1,0,1,1,0,1,1,0,1,1,0,1,0,0,1,0)$	7,14,18	8,9,15,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,1,0,0,0,0,1,1,1) \xrightarrow{1r} (0,1,0,0,1,0,0,1,0,0,1,0,1,1,0,0)$	7,14,16,17	8,9,15,17	2^{-23}
$(0,0,0,0,0,0,1,1,1,0,0,0,1,0,0,0) \xrightarrow{1r} (0,1,1,1,1,1,1,0,1,1,1,0,1,1,0,1)$	7,17	8,9,13,17	$2^{-28.5}$
$(0,0,0,0,0,0,1,1,1,0,0,0,1,0,0,1) \xrightarrow{1r} (1,0,0,0,0,0,0,1,0,0,0,1,0,0,1,1)$	7,16,18	8,9,13,18	2^{-12}
$(0,0,0,0,0,0,1,1,1,0,0,0,1,0,1,0) \xrightarrow{1r} (1,0,1,1,1,1,1,1,1,1,0,1,1,0,1,1)$	7,17,18	8,9,13,15,17,18	$2^{-28.5}$
$(0,0,0,0,0,0,1,1,1,0,0,0,1,0,1,1) \xrightarrow{1r} (0,1,0,0,0,0,0,0,0,0,0,1,0,0,1,1)$	7,16	8,9,13,15	2^{-12}
$(0,0,0,0,0,0,1,1,1,0,0,0,1,1,0,0) \xrightarrow{1r} (1,0,1,0,0,0,1,1,1,0,0,1,0,0,1,0)$	7,14,18	8,9,13,18	2^{-23}
$(0,0,0,0,0,0,1,1,1,0,0,0,1,1,0,1) \xrightarrow{1r} (0,1,0,1,1,1,0,0,0,1,1,0,1,1,0,0)$	7,14,16,17	8,9,13,17	$2^{-28.5}$
$(0,0,0,0,0,0,1,1,1,0,0,0,1,1,1,0) \xrightarrow{1r} (0,1,1,0,0,0,1,0,1,0,0,1,0,0,1,0)$	7,14	8,9,13,15	2^{-23}
$(0,0,0,0,0,0,1,1,1,0,0,0,1,1,1,1) \xrightarrow{1r} (1,0,0,1,1,1,0,1,0,1,1,0,1,1,0,0)$	7,14,16,17,18	8,9,13,15,17,18	$2^{-28.5}$
$(0,0,0,0,0,0,1,1,1,0,0,1,0,0,0,0) \xrightarrow{1r} (0,1,1,1,0,1,0,1,1,1,1,1,0,0,1,0)$	7,12	8,9	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,1,0,0,1,0,0,0,1) \xrightarrow{1r} (1,0,0,0,1,0,1,0,0,0,0,0,1,1,0,0)$	7,12,16,17,18	8,9,17,18	2^{-12}
$(0,0,0,0,0,0,1,1,1,0,0,1,0,0,1,0) \xrightarrow{1r} (1,0,1,1,0,1,0,0,1,1,1,1,0,0,1,0)$	7,12,18	8,9,15,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,1,0,0,1,0,0,1,1) \xrightarrow{1r} (0,1,0,0,1,0,1,1,0,0,0,0,1,1,0,0)$	7,12,16,17	8,9,15,17	2^{-12}
$(0,0,0,0,0,0,1,1,1,0,0,1,0,1,0,0) \xrightarrow{1r} (1,0,1,0,1,0,0,0,1,0,0,0,1,1,0,1)$	7,12,14,17,18	8,9,17,18	2^{-23}
$(0,0,0,0,0,0,1,1,1,0,0,1,0,1,0,1) \xrightarrow{1r} (0,1,0,1,0,1,1,1,0,1,1,1,0,0,1,1)$	7,12,14,16	8,9	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,1,0,0,1,0,1,1,0) \xrightarrow{1r} (0,1,1,0,1,0,0,1,1,0,0,0,1,1,0,1)$	7,12,14,17	8,9,15,17	2^{-23}
$(0,0,0,0,0,0,1,1,1,0,0,1,0,1,1,1) \xrightarrow{1r} (1,0,0,1,0,1,1,0,0,1,1,1,0,0,1,1)$	7,12,14,16,18	8,9,15,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,1,0,0,1,1,0,0,0) \xrightarrow{1r} (1,0,1,0,0,0,0,1,1,0,1,1,0,0,1,0)$	7,12,18	8,9,13,18	2^{-23}
$(0,0,0,0,0,0,1,1,1,0,0,1,1,0,0,1) \xrightarrow{1r} (0,1,0,1,1,1,1,0,0,1,0,0,1,1,0,0)$	7,12,16,17	8,9,13,17	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,1,0,0,1,1,0,1,0) \xrightarrow{1r} (0,1,1,0,0,0,0,0,1,0,1,1,0,0,1,0)$	7,12	8,9,13,15	2^{-23}
$(0,0,0,0,0,0,1,1,1,0,0,1,1,0,1,1) \xrightarrow{1r} (1,0,0,1,1,1,1,1,0,1,0,0,1,1,0,0)$	7,12,16,17,18	8,9,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,1,0,0,1,1,1,0,0) \xrightarrow{1r} (0,1,1,1,1,1,0,0,1,1,0,0,1,1,0,1)$	7,12,14,17	8,9,13,17	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,1,0,0,1,1,1,0,1) \xrightarrow{1r} (1,0,0,0,0,0,1,1,0,0,1,1,0,0,1,1)$	7,12,14,16,18	8,9,13,18	2^{-12}
$(0,0,0,0,0,0,1,1,1,0,0,1,1,1,1,0) \xrightarrow{1r} (1,0,1,1,1,1,0,1,1,1,0,0,1,1,0,1)$	7,12,14,17,18	8,9,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,1,0,0,1,1,1,1,1) \xrightarrow{1r} (0,1,0,0,0,0,1,0,0,0,1,1,0,0,1,1)$	7,12,14,16	8,9,13,15	2^{-12}

Table 0.30 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,0,0,1,1,1,0,1,0,0,0,0,0) \xrightarrow{1r} (0,1,1,0,1,1,1,0,1,1,1,1,1,1,0,1)$	7,17	8,9,11,17	2^{-23}
$(0,0,0,0,0,0,1,1,1,0,1,0,0,0,0,1) \xrightarrow{1r} (1,0,0,1,0,0,0,1,0,0,0,0,0,0,1,1)$	7,16,18	8,9,11,18	$2^{-6.5}$
$(0,0,0,0,0,0,1,1,1,0,1,0,0,0,1,0) \xrightarrow{1r} (1,0,1,0,1,1,1,1,1,1,1,1,1,1,0,1)$	7,17,18	8,9,11,15,17,18	2^{-23}
$(0,0,0,0,0,0,1,1,1,0,1,0,0,0,1,1) \xrightarrow{1r} (0,1,0,1,0,0,0,0,0,0,0,0,0,0,1,1)$	7,16	8,9,11,15	$2^{-6.5}$
$(0,0,0,0,0,0,1,1,1,0,1,0,0,1,0,0) \xrightarrow{1r} (1,0,1,1,0,0,1,1,1,0,0,0,0,0,1,0)$	7,14,18	8,9,11,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,1,0,1,0,0,1,0,1) \xrightarrow{1r} (0,1,0,0,1,1,0,0,0,1,1,1,1,1,0,0)$	7,14,16,17	8,9,11,17	2^{-23}
$(0,0,0,0,0,0,1,1,1,0,1,0,0,1,1,0) \xrightarrow{1r} (0,1,1,1,0,0,1,0,1,0,0,0,0,0,1,0)$	7,14	8,9,11,15	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,1,0,1,0,0,1,1,1) \xrightarrow{1r} (1,0,0,0,1,1,0,1,0,1,1,1,1,1,0,0)$	7,14,16,17,18	8,9,11,15,17,18	2^{-23}
$(0,0,0,0,0,0,1,1,1,0,1,0,1,0,0,0) \xrightarrow{1r} (1,0,1,1,1,0,1,0,1,0,1,1,1,1,0,1)$	7,17,18	8,9,11,13,17,18	$2^{-28.5}$
$(0,0,0,0,0,0,1,1,1,0,1,0,1,0,0,1) \xrightarrow{1r} (0,1,0,0,0,1,0,1,0,1,0,0,0,0,1,1)$	7,16	8,9,11,13	2^{-12}
$(0,0,0,0,0,0,1,1,1,0,1,0,1,0,1,0) \xrightarrow{1r} (0,1,1,1,1,0,1,1,1,0,1,1,1,1,0,1)$	7,17	8,9,11,13,15,17	$2^{-28.5}$
$(0,0,0,0,0,0,1,1,1,0,1,0,1,0,1,1) \xrightarrow{1r} (1,0,0,0,0,1,0,0,0,1,0,0,0,0,1,1)$	7,16,18	8,9,11,13,15,18	2^{-12}
$(0,0,0,0,0,0,1,1,1,0,1,0,1,1,0,0) \xrightarrow{1r} (0,1,1,0,0,1,1,1,1,1,0,0,0,0,1,0)$	7,14	8,9,11,13	2^{-12}
$(0,0,0,0,0,0,1,1,1,0,1,0,1,1,0,1) \xrightarrow{1r} (1,0,0,1,1,0,0,0,0,0,1,1,1,1,0,0)$	7,14,16,17,18	8,9,11,13,17,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,1,0,1,0,1,1,1,0) \xrightarrow{1r} (1,0,1,0,0,1,1,0,1,1,0,0,0,0,1,0)$	7,14,18	8,9,11,13,15,18	2^{-12}
$(0,0,0,0,0,0,1,1,1,0,1,0,1,1,1,1) \xrightarrow{1r} (0,1,0,1,1,0,0,1,0,0,1,1,1,1,0,0)$	7,14,16,17	8,9,11,13,15,17	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,1,0,1,1,0,0,0,0) \xrightarrow{1r} (1,0,1,1,0,0,0,1,1,0,1,0,0,0,1,0)$	7,12,18	8,9,11,18	$2^{-28.5}$
$(0,0,0,0,0,0,1,1,1,0,1,1,0,0,0,1) \xrightarrow{1r} (0,1,0,0,1,1,1,0,0,1,0,1,1,1,0,0)$	7,12,16,17	8,9,11,17	2^{-23}
$(0,0,0,0,0,0,1,1,1,0,1,1,0,0,1,0) \xrightarrow{1r} (0,1,1,1,0,0,0,0,1,0,1,0,0,0,1,0)$	7,12	8,9,11,15	$2^{-28.5}$
$(0,0,0,0,0,0,1,1,1,0,1,1,0,0,1,1) \xrightarrow{1r} (1,0,0,0,1,1,1,1,0,1,0,1,1,1,0,0)$	7,12,16,17,18	8,9,11,15,17,18	2^{-23}
$(0,0,0,0,0,0,1,1,1,0,1,1,0,1,0,0) \xrightarrow{1r} (0,1,1,0,1,1,0,0,1,1,0,1,1,1,0,1)$	7,12,14,17	8,9,11,17	2^{-23}
$(0,0,0,0,0,0,1,1,1,0,1,1,0,1,0,1) \xrightarrow{1r} (1,0,0,1,0,0,1,1,0,0,1,0,0,0,1,1)$	7,12,14,16,18	8,9,11,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,1,0,1,1,0,1,1,0) \xrightarrow{1r} (1,0,1,0,1,1,0,1,1,1,0,1,1,1,0,1)$	7,12,14,17,18	8,9,11,15,17,18	2^{-23}
$(0,0,0,0,0,0,1,1,1,0,1,1,0,1,1,1) \xrightarrow{1r} (0,1,0,1,0,0,1,0,0,0,1,0,0,0,1,1)$	7,12,14,16	8,9,11,15	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,1,0,1,1,1,0,0,0) \xrightarrow{1r} (0,1,1,0,0,1,0,1,1,1,1,0,0,0,1,0)$	7,12	8,9,11,13	2^{-23}
$(0,0,0,0,0,0,1,1,1,0,1,1,1,0,0,1) \xrightarrow{1r} (1,0,0,1,1,0,1,0,0,0,0,1,1,1,0,0)$	7,12,16,17,18	8,9,11,13,17,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,1,0,1,1,1,0,1,0) \xrightarrow{1r} (1,0,1,0,0,1,0,0,1,1,1,0,0,0,1,0)$	7,12,18	8,9,11,13,15,18	2^{-23}
$(0,0,0,0,0,0,1,1,1,0,1,1,1,0,1,1) \xrightarrow{1r} (0,1,0,1,1,0,1,1,0,0,0,1,1,1,0,0)$	7,12,16,17	8,9,11,13,15,17	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,1,0,1,1,1,1,0,0) \xrightarrow{1r} (1,0,1,1,1,0,0,0,1,0,0,1,1,1,0,1)$	7,12,14,17,18	8,9,11,13,17,18	$2^{-28.5}$
$(0,0,0,0,0,0,1,1,1,0,1,1,1,1,0,1) \xrightarrow{1r} (0,1,0,0,0,1,1,1,0,1,1,0,0,0,1,1)$	7,12,14,16	8,9,11,13	2^{-23}
$(0,0,0,0,0,0,1,1,1,0,1,1,1,1,1,0) \xrightarrow{1r} (0,1,1,1,1,0,0,1,1,0,0,1,1,1,0,1)$	7,12,14,17	8,9,11,13,15,17	$2^{-28.5}$
$(0,0,0,0,0,0,1,1,1,0,1,1,1,1,1,1) \xrightarrow{1r} (1,0,0,0,0,1,1,0,0,1,1,0,0,0,1,1)$	7,12,14,16,18	8,9,11,13,15,18	2^{-23}

Table 0.31 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,0,0,1,1,1,1,0,0,0,0,0,0) \xrightarrow{1r} (0,1,0,1,1,1,1,1,1,1,1,1,0,1,0)$	7,10	8,9	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,1,1,0,0,0,0,0,1) \xrightarrow{1r} (1,0,1,0,0,0,0,0,0,0,0,0,0,1,0,0)$	7,10,16,17,18	8,9,17,18	2^{-1}
$(0,0,0,0,0,0,1,1,1,1,0,0,0,0,1,0) \xrightarrow{1r} (1,0,0,1,1,1,1,0,1,1,1,1,1,0,1,0)$	7,10,18	8,9,15,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,1,1,0,0,0,0,1,1) \xrightarrow{1r} (0,1,1,0,0,0,0,1,0,0,0,0,0,1,0,0)$	7,10,16,17	8,9,15,17	2^{-1}
$(0,0,0,0,0,0,1,1,1,1,0,0,0,1,0,0) \xrightarrow{1r} (1,0,0,0,0,0,1,0,1,0,0,0,0,1,0,1)$	7,10,14,17,18	8,9,17,18	2^{-12}
$(0,0,0,0,0,0,1,1,1,1,0,0,0,1,0,1) \xrightarrow{1r} (0,1,1,1,1,1,0,1,0,1,1,1,1,0,1,1)$	7,10,14,16	8,9	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,1,1,0,0,0,1,1,0) \xrightarrow{1r} (0,1,0,0,0,0,1,1,1,0,0,0,0,1,0,1)$	7,10,14,17	8,9,15,17	2^{-12}
$(0,0,0,0,0,0,1,1,1,1,0,0,0,1,1,1) \xrightarrow{1r} (1,0,1,1,1,1,0,0,0,1,1,1,1,0,1,1)$	7,10,14,16,18	8,9,15,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,1,1,0,0,1,0,0,0) \xrightarrow{1r} (1,0,0,0,1,0,1,1,1,0,1,1,1,0,1,0)$	7,10,18	8,9,13,18	2^{-23}
$(0,0,0,0,0,0,1,1,1,1,0,0,1,0,0,1) \xrightarrow{1r} (0,1,1,1,0,1,0,0,0,1,0,0,0,1,0,0)$	7,10,16,17	8,9,13,17	$2^{-6.5}$
$(0,0,0,0,0,0,1,1,1,1,0,0,1,0,1,0) \xrightarrow{1r} (0,1,0,0,1,0,1,0,1,0,1,0,1,1,0,1,0)$	7,10	8,9,13,15	2^{-23}
$(0,0,0,0,0,0,1,1,1,1,0,0,1,0,1,1) \xrightarrow{1r} (1,0,1,1,0,1,0,1,0,1,0,1,0,0,0,1,0,0)$	7,10,16,17,18	8,9,13,15,17,18	$2^{-6.5}$
$(0,0,0,0,0,0,1,1,1,1,0,0,1,1,0,0) \xrightarrow{1r} (0,1,0,1,0,1,1,0,1,1,0,0,0,1,0,1)$	7,10,14,17	8,9,13,17	$2^{-6.5}$
$(0,0,0,0,0,0,1,1,1,1,0,0,1,1,0,1) \xrightarrow{1r} (1,0,1,0,1,0,0,1,0,0,1,1,1,0,1,1)$	7,10,14,16,18	8,9,13,18	2^{-12}
$(0,0,0,0,0,0,1,1,1,1,0,0,1,1,1,0) \xrightarrow{1r} (1,0,0,1,0,1,1,1,1,1,0,0,0,1,0,1)$	7,10,14,17,18	8,9,13,15,17,18	$2^{-6.5}$
$(0,0,0,0,0,0,1,1,1,1,0,0,1,1,1,1) \xrightarrow{1r} (0,1,1,0,1,0,0,0,0,0,1,1,1,0,1,1)$	7,10,14,16	8,9,13,15	2^{-12}
$(0,0,0,0,0,0,1,1,1,1,0,1,0,0,0,0) \xrightarrow{1r} (1,0,0,0,0,0,0,0,1,0,1,0,0,1,0,1)$	7,10,12,17,18	8,9,17,18	2^{-23}
$(0,0,0,0,0,0,1,1,1,1,0,1,0,0,0,1) \xrightarrow{1r} (0,1,1,1,1,1,1,0,1,0,1,1,0,1,1,1)$	7,10,12,16	8,9	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,1,1,0,1,0,0,1,0) \xrightarrow{1r} (0,1,0,0,0,0,0,1,1,0,1,0,0,1,0,1)$	7,10,12,17	8,9,15,17	2^{-23}
$(0,0,0,0,0,0,1,1,1,1,0,1,0,0,1,1) \xrightarrow{1r} (1,0,1,1,1,1,1,0,0,1,0,1,1,0,1,1)$	7,10,12,16,18	8,9,15,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,1,1,0,1,0,1,0,0) \xrightarrow{1r} (0,1,0,1,1,1,0,1,1,1,0,1,1,0,1,0)$	7,10,12,14	8,9	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,1,1,0,1,0,1,0,1) \xrightarrow{1r} (1,0,1,0,0,0,1,0,0,0,1,0,0,1,0,0)$	7,10,12,14,16,17,18	8,9,17,18	2^{-12}
$(0,0,0,0,0,0,1,1,1,1,0,1,0,1,1,0) \xrightarrow{1r} (1,0,0,1,1,1,0,0,1,1,0,1,1,0,1,0)$	7,10,12,14,18	8,9,15,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,1,1,0,1,0,1,1,1) \xrightarrow{1r} (0,1,1,0,0,0,1,1,0,0,1,0,0,1,0,0)$	7,10,12,14,16,17	8,9,15,17	2^{-12}
$(0,0,0,0,0,0,1,1,1,1,0,1,0,1,1,0) \xrightarrow{1r} (0,1,0,1,0,1,0,0,1,1,1,1,0,0,1,0,1)$	7,10,12,17	8,9,13,17	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,1,1,0,1,1,0,0,1) \xrightarrow{1r} (1,0,1,0,1,0,1,1,1,0,0,0,1,1,0,1,1)$	7,10,12,16,18	8,9,13,18	2^{-12}
$(0,0,0,0,0,0,1,1,1,1,0,1,1,0,1,0) \xrightarrow{1r} (1,0,0,1,0,1,0,1,1,1,1,0,0,1,0,1)$	7,10,12,17,18	8,9,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,1,1,0,1,1,0,1,1) \xrightarrow{1r} (0,1,1,0,1,0,1,0,0,0,0,1,1,0,1,1)$	7,10,12,16	8,9,13,15	2^{-12}
$(0,0,0,0,0,0,1,1,1,1,0,1,1,1,0,0) \xrightarrow{1r} (1,0,0,0,1,0,0,1,1,0,0,1,1,0,1,0)$	7,10,12,14,18	8,9,13,18	2^{-23}
$(0,0,0,0,0,0,1,1,1,1,0,1,1,1,0,1) \xrightarrow{1r} (0,1,1,1,0,1,1,0,0,1,1,0,0,1,0,0)$	7,10,12,14,16,17	8,9,13,17	$2^{-17.5}$
$(0,0,0,0,0,0,1,1,1,1,0,1,1,1,1,0) \xrightarrow{1r} (0,1,0,0,1,0,0,0,1,0,0,1,1,0,1,0)$	7,10,12,14	8,9,13,15	2^{-23}
$(0,0,0,0,0,0,1,1,1,1,0,1,1,1,1,1) \xrightarrow{1r} (1,0,1,1,0,1,1,1,0,1,1,0,0,1,0,0)$	7,10,12,14,16,17,18	8,9,13,15,17,18	$2^{-17.5}$

Table 0.32 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	7,10,18	8,9,11,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	7,10,16,17	8,9,11,17	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	7,10	8,9,11,15	$2^{-28.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	7,10,16,17,18	8,9,11,15,17,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	7,10,14,17	8,9,11,17	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	7,10,14,16,18	8,9,11,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	7,10,14,17,18	8,9,11,15,17,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	7,10,14,16	8,9,11,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	7,10	8,9,11,13	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	7,10,16,17,18	8,9,11,13,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	7,10,18	8,9,11,13,15,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	7,10,16,17	8,9,11,13,15,17	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	7,10,14,17,18	8,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	7,10,14,16	8,9,11,13	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	7,10,14,17	8,9,11,13,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	7,10,14,16,18	8,9,11,13,15,18	2^{-23}
$(0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	7,10,12,17	8,9,11,17	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	7,10,12,16,18	8,9,11,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	7,10,12,17,18	8,9,11,15,17,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	7,10,12,16	8,9,11,15	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	7,10,12,14,18	8,9,11,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	7,10,12,14,16,17	8,9,11,17	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	7,10,12,14	8,9,11,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	7,10,12,14,16,17,18	8,9,11,15,17,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	7,10,12,17,18	8,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	7,10,12,16	8,9,11,13	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	7,10,12,17	8,9,11,13,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	7,10,12,16,18	8,9,11,13,15,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	7,10,12,14	8,9,11,13	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	7,10,12,14,16,17,18	8,9,11,13,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	7,10,12,14,18	8,9,11,13,15,18	2^{-12}
$(0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	7,10,12,14,16,17	8,9,11,13,15,17	$2^{-6.5}$

Table 0.33 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (1,1,0,1,1,1,1,1,0,1,1,1,0,1,1,1)$	17,18	6,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,1) \xrightarrow{1r} (0,0,1,0,0,0,0,0,1,0,0,0,1,0,0,1)$	16	6	2^{-12}
$(0,0,0,0,0,1,0,0,0,0,0,0,0,0,1,0) \xrightarrow{1r} (0,0,0,1,1,1,1,0,0,1,1,1,0,1,1,1)$	17	6,15,17	$2^{-17.5}$
$(0,0,0,0,0,1,0,0,0,0,0,0,0,0,1,1) \xrightarrow{1r} (1,1,1,0,0,0,0,1,1,0,0,0,1,0,0,1)$	16,18	6,15,18	2^{-12}
$(0,0,0,0,0,1,0,0,0,0,0,0,0,1,0,0) \xrightarrow{1r} (0,0,0,0,0,0,1,0,0,0,0,0,1,0,0,0)$	14	6	2^{-1}
$(0,0,0,0,0,1,0,0,0,0,0,0,0,1,0,1) \xrightarrow{1r} (1,1,1,1,1,1,0,1,1,1,1,1,0,1,1,0)$	14,16,17,18	6,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,0,0,0,0,0,0,0,1,1,0) \xrightarrow{1r} (1,1,0,0,0,0,1,1,0,0,0,0,1,0,0,0)$	14,18	6,15,18	2^{-1}
$(0,0,0,0,0,1,0,0,0,0,0,0,0,1,1,1) \xrightarrow{1r} (0,0,1,1,1,1,0,0,1,1,1,1,0,1,1,0)$	14,16,17	6,15,17	$2^{-17.5}$
$(0,0,0,0,0,1,0,0,0,0,0,0,1,0,0,0) \xrightarrow{1r} (0,0,0,0,1,0,1,1,0,0,1,1,0,1,1,1)$	17	6,13,17	2^{-12}
$(0,0,0,0,0,1,0,0,0,0,0,0,1,0,0,1) \xrightarrow{1r} (1,1,1,1,0,1,0,0,1,1,0,0,1,0,0,1)$	16,18	6,13,18	$2^{-6.5}$
$(0,0,0,0,0,1,0,0,0,0,0,0,0,1,0,1) \xrightarrow{1r} (1,1,0,0,1,0,1,0,0,0,1,1,0,1,1,1)$	17,18	6,13,15,17,18	2^{-12}
$(0,0,0,0,0,1,0,0,0,0,0,0,0,1,0,1) \xrightarrow{1r} (0,0,1,1,0,1,0,1,1,1,1,0,0,1,0,0,1)$	16	6,13,15	$2^{-6.5}$
$(0,0,0,0,0,1,0,0,0,0,0,0,0,1,1,0,0) \xrightarrow{1r} (1,1,0,1,0,1,1,0,0,1,0,0,1,0,0,0,0)$	14,18	6,13,18	$2^{-6.5}$
$(0,0,0,0,0,1,0,0,0,0,0,0,0,1,1,0,1) \xrightarrow{1r} (0,0,1,0,1,0,0,1,1,0,1,1,0,1,1,0)$	14,16,17	6,13,17	2^{-23}
$(0,0,0,0,0,1,0,0,0,0,0,0,0,1,1,1,0) \xrightarrow{1r} (0,0,0,1,0,1,1,1,0,1,0,0,1,0,0,0,0)$	14	6,13,15	$2^{-6.5}$
$(0,0,0,0,0,1,0,0,0,0,0,0,0,1,1,1,1) \xrightarrow{1r} (1,1,1,0,1,0,0,0,1,0,1,1,0,1,1,0)$	14,16,17,18	6,13,15,17,18	2^{-23}
$(0,0,0,0,0,1,0,0,0,0,0,0,1,0,0,0,0) \xrightarrow{1r} (0,0,0,0,0,0,0,0,0,0,0,1,0,1,0,0,0)$	12	6	2^{-12}
$(0,0,0,0,0,1,0,0,0,0,0,0,1,0,0,0,1) \xrightarrow{1r} (1,1,1,1,1,1,1,1,1,1,0,1,0,1,1,0)$	12,16,17,18	6,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,0,0,0,0,0,0,1,0,0,1,0) \xrightarrow{1r} (1,1,0,0,0,0,0,1,0,0,1,0,1,0,1,0,0)$	12,18	6,15,18	2^{-12}
$(0,0,0,0,0,1,0,0,0,0,0,0,1,0,0,1,1) \xrightarrow{1r} (0,0,1,1,1,1,1,0,1,1,0,1,1,0,1,1,0)$	12,16,17	6,15,17	$2^{-17.5}$
$(0,0,0,0,0,1,0,0,0,0,0,0,1,0,1,0,0) \xrightarrow{1r} (1,1,0,1,1,1,0,1,0,1,0,1,0,1,1,1,1)$	12,14,17,18	6,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,0,0,0,0,0,0,1,0,1,0,1) \xrightarrow{1r} (0,0,1,0,0,0,1,0,1,0,1,0,1,0,1,0,0,1)$	12,14,16	6	2^{-23}
$(0,0,0,0,0,1,0,0,0,0,0,0,1,0,1,1,0) \xrightarrow{1r} (0,0,0,1,1,1,0,0,0,1,0,1,0,1,0,1,1,1)$	12,14,17	6,15,17	$2^{-17.5}$
$(0,0,0,0,0,1,0,0,0,0,0,0,1,0,1,1,1) \xrightarrow{1r} (1,1,1,0,0,0,1,1,1,0,1,0,1,0,1,0,0,1)$	12,14,16,18	6,15,18	2^{-23}
$(0,0,0,0,0,1,0,0,0,0,0,0,1,1,0,0,0) \xrightarrow{1r} (1,1,0,1,0,1,0,0,0,1,1,0,1,0,1,0,0,0)$	12,18	6,13,18	$2^{-17.5}$
$(0,0,0,0,0,1,0,0,0,0,0,0,1,1,0,0,1) \xrightarrow{1r} (0,0,1,0,1,0,1,1,1,0,0,1,0,0,1,0,1,0)$	12,16,17	6,13,17	2^{-23}
$(0,0,0,0,0,1,0,0,0,0,0,0,1,1,0,1,0) \xrightarrow{1r} (0,0,0,1,0,1,0,1,0,1,0,1,1,0,1,0,0,0)$	12	6,13,15	$2^{-17.5}$
$(0,0,0,0,0,1,0,0,0,0,0,0,1,1,0,1,1) \xrightarrow{1r} (1,1,1,0,1,0,1,0,1,0,1,0,0,1,0,1,1,0)$	12,16,17,18	6,13,15,17,18	2^{-23}
$(0,0,0,0,0,1,0,0,0,0,0,0,1,1,1,0,0) \xrightarrow{1r} (0,0,0,0,1,0,0,1,0,0,0,1,0,0,1,1,1,1)$	12,14,17	6,13,17	2^{-12}
$(0,0,0,0,0,1,0,0,0,0,0,0,1,1,1,0,1) \xrightarrow{1r} (1,1,1,1,0,1,1,0,1,1,1,1,0,1,0,0,1)$	12,14,16,18	6,13,18	$2^{-17.5}$
$(0,0,0,0,0,1,0,0,0,0,0,0,1,1,1,1,0) \xrightarrow{1r} (1,1,0,0,1,0,0,0,0,0,0,0,1,0,1,1,1,1)$	12,14,17,18	6,13,15,17,18	2^{-12}
$(0,0,0,0,0,1,0,0,0,0,0,0,1,1,1,1,1) \xrightarrow{1r} (0,0,1,1,0,1,1,1,1,1,1,1,0,1,0,0,1)$	12,14,16	6,13,15	$2^{-17.5}$

Table 0.34 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	17	6,11,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	16,18	6,11,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	17,18	6,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	16	6,11,15	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	14,18	6,11,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	14,16,17	6,11,17	$2^{-28.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	14	6,11,15	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	14,16,17,18	6,11,15,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	17,18	6,11,13,17,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	16	6,11,13	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	17	6,11,13,15,17	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	16,18	6,11,13,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	14	6,11,13	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	14,16,17,18	6,11,13,17,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	14,18	6,11,13,15,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	14,16,17	6,11,13,15,17	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	12,18	6,11,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	12,16,17	6,11,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	12	6,11,15	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	12,16,17,18	6,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	12,14,17	6,11,17	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	12,14,16,18	6,11,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	12,14,17,18	6,11,15,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	12,14,16	6,11,15	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	12	6,11,13	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	12,16,17,18	6,11,13,17,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	12,18	6,11,13,15,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	12,16,17	6,11,13,15,17	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	12,14,17,18	6,11,13,17,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	12,14,16	6,11,13	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	12,14,17	6,11,13,15,17	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	12,14,16,18	6,11,13,15,18	$2^{-17.5}$

Table 0.35 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	10	6	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	10,16,17,18	6,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	10,18	6,15,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	10,16,17	6,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	10,14,17,18	6,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	10,14,16	6	2^{-34}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	10,14,17	6,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	10,14,16,18	6,15,18	2^{-34}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	10,18	6,13,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	10,16,17	6,13,17	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	10	6,13,15	$2^{-28.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	10,16,17,18	6,13,15,17,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	10,14,17	6,13,17	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	10,14,16,18	6,13,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	10,14,17,18	6,13,15,17,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	10,14,16	6,13,15	$2^{-28.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	10,12,17,18	6,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	10,12,16	6	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	10,12,17	6,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	10,12,16,18	6,15,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	10,12,14	6	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	10,12,14,16,17,18	6,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	10,12,14,18	6,15,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	10,12,14,16,17	6,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	10,12,17	6,13,17	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	10,12,16,18	6,13,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	10,12,17,18	6,13,15,17,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	10,12,16	6,13,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	10,12,14,18	6,13,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	10,12,14,16,17	6,13,17	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	10,12,14	6,13,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	10,12,14,16,17,18	6,13,15,17,18	2^{-23}

Table 0.36 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	10,18	6,11,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	10,16,17	6,11,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	10	6,11,15	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	10,16,17,18	6,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	10,14,17	6,11,17	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	10,14,16,18	6,11,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	10,14,17,18	6,11,15,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	10,14,16	6,11,15	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	10	6,11,13	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	10,16,17,18	6,11,13,17,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	10,18	6,11,13,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	10,16,17	6,11,13,15,17	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	10,14,17,18	6,11,13,17,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	10,14,16	6,11,13	$2^{-28.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	10,14,17	6,11,13,15,17	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	10,14,16,18	6,11,13,15,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	10,12,17	6,11,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	10,12,16,18	6,11,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	10,12,17,18	6,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	10,12,16	6,11,15	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	10,12,14,18	6,11,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	10,12,14,16,17	6,11,17	$2^{-28.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	10,12,14	6,11,15	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	10,12,14,16,17,18	6,11,15,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	10,12,17,18	6,11,13,17,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	10,12,16	6,11,13	$2^{-28.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	10,12,17	6,11,13,15,17	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	10,12,16,18	6,11,13,15,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	10,12,14	6,11,13	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	10,12,14,16,17,18	6,11,13,17,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	10,12,14,18	6,11,13,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	10,12,14,16,17	6,11,13,15,17	2^{-23}

Table 0.37 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	17	6,9,17	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	16,18	6,9,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	17,18	6,9,15,17,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	16	6,9,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	14,18	6,9,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	14,16,17	6,9,17	2^{-34}
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	14	6,9,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	14,16,17,18	6,9,15,17,18	2^{-34}
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	17,18	6,9,13,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	16	6,9,13	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	17	6,9,13,15,17	$2^{-28.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	16,18	6,9,13,15,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	14	6,9,13	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	14,16,17,18	6,9,13,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	14,18	6,9,13,15,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	14,16,17	6,9,13,15,17	$2^{-28.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	12,18	6,9,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	12,16,17	6,9,17	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	12	6,9,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	12,16,17,18	6,9,15,17,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	12,14,17	6,9,17	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	12,14,16,18	6,9,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	12,14,17,18	6,9,15,17,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	12,14,16	6,9,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	12	6,9,13	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	12,16,17,18	6,9,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	12,18	6,9,13,15,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	12,16,17	6,9,13,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	12,14,17,18	6,9,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	12,14,16	6,9,13	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	12,14,17	6,9,13,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	12,14,16,18	6,9,13,15,18	2^{-23}

Table 0.38 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,0,1,0,0,1,0,1,0,0,0,0,0) \xrightarrow{1r} (1,0,0,0,1,1,1,0,0,1,1,1,0,0,1,1)$	17,18	6,9,11,17,18	2^{-23}
$(0,0,0,0,0,1,0,0,1,0,1,0,0,0,0,1) \xrightarrow{1r} (0,1,1,1,0,0,0,1,1,0,0,0,1,1,0,1)$	16	6,9,11	$2^{-17.5}$
$(0,0,0,0,0,1,0,0,1,0,1,0,0,0,1,0) \xrightarrow{1r} (0,1,0,0,1,1,1,1,0,1,1,1,0,0,1,1)$	17	6,9,11,15,17	2^{-23}
$(0,0,0,0,0,1,0,0,1,0,1,0,0,0,1,1) \xrightarrow{1r} (1,0,1,1,0,0,0,0,1,0,0,0,1,1,0,1)$	16,18	6,9,11,15,18	$2^{-17.5}$
$(0,0,0,0,0,1,0,0,1,0,1,0,0,1,0,0) \xrightarrow{1r} (0,1,0,1,0,0,1,1,0,0,0,0,1,1,0,0)$	14	6,9,11	$2^{-6.5}$
$(0,0,0,0,0,1,0,0,1,0,1,0,0,1,0,1) \xrightarrow{1r} (1,0,1,0,1,1,0,0,1,1,1,1,0,0,1,0)$	14,16,17,18	6,9,11,17,18	2^{-23}
$(0,0,0,0,0,1,0,0,1,0,1,0,0,1,1,0) \xrightarrow{1r} (1,0,0,1,0,0,1,0,0,0,0,0,1,1,0,0)$	14,18	6,9,11,15,18	$2^{-6.5}$
$(0,0,0,0,0,1,0,0,1,0,1,0,0,1,1,1) \xrightarrow{1r} (0,1,1,0,1,1,0,1,1,1,1,1,0,0,1,0)$	14,16,17	6,9,11,15,17	2^{-23}
$(0,0,0,0,0,1,0,0,1,0,1,0,1,0,0,0) \xrightarrow{1r} (0,1,0,1,1,0,1,0,0,0,1,1,0,0,1,1)$	17	6,9,11,13,17	$2^{-17.5}$
$(0,0,0,0,0,1,0,0,1,0,1,0,1,0,0,1) \xrightarrow{1r} (1,0,1,0,0,1,0,1,1,1,0,0,1,1,0,1)$	16,18	6,9,11,13,18	2^{-12}
$(0,0,0,0,0,1,0,0,1,0,1,0,1,0,1,0) \xrightarrow{1r} (1,0,0,1,1,0,1,1,0,0,1,1,0,0,1,1)$	17,18	6,9,11,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,0,0,1,0,1,0,1,0,1,1) \xrightarrow{1r} (0,1,1,0,0,1,0,0,1,1,0,0,1,1,0,1)$	16	6,9,11,13,15	2^{-12}
$(0,0,0,0,0,1,0,0,1,0,1,0,1,1,0,0) \xrightarrow{1r} (1,0,0,0,0,1,1,1,0,1,0,0,1,1,0,0)$	14,18	6,9,11,13,18	2^{-12}
$(0,0,0,0,0,1,0,0,1,0,1,0,1,1,0,1) \xrightarrow{1r} (0,1,1,1,1,0,0,0,1,0,1,1,0,0,1,0)$	14,16,17	6,9,11,13,17	$2^{-28.5}$
$(0,0,0,0,0,1,0,0,1,0,1,0,1,1,1,0) \xrightarrow{1r} (0,1,0,0,0,1,1,0,0,1,0,0,1,1,0,0)$	14	6,9,11,13,15	2^{-12}
$(0,0,0,0,0,1,0,0,1,0,1,0,1,1,1,1) \xrightarrow{1r} (1,0,1,1,1,0,0,1,1,0,1,1,0,0,1,0)$	14,16,17,18	6,9,11,13,15,17,18	$2^{-28.5}$
$(0,0,0,0,0,1,0,0,1,0,1,0,0,0,0) \xrightarrow{1r} (0,1,0,1,0,0,0,1,0,0,1,0,1,1,0,0)$	12	6,9,11	$2^{-17.5}$
$(0,0,0,0,0,1,0,0,1,0,1,1,0,0,0,1) \xrightarrow{1r} (1,0,1,0,1,1,1,0,1,1,0,1,0,0,1,0)$	12,16,17,18	6,9,11,17,18	2^{-23}
$(0,0,0,0,0,1,0,0,1,0,1,1,0,0,1,0) \xrightarrow{1r} (1,0,0,1,0,0,0,0,0,0,1,0,1,1,0,0)$	12,18	6,9,11,15,18	$2^{-17.5}$
$(0,0,0,0,0,1,0,0,1,0,1,1,0,0,1,1) \xrightarrow{1r} (0,1,1,0,1,1,1,1,1,1,0,1,0,0,1,0)$	12,16,17	6,9,11,15,17	2^{-23}
$(0,0,0,0,0,1,0,0,1,0,1,1,0,1,0,0) \xrightarrow{1r} (1,0,0,0,1,1,0,0,0,1,0,1,0,0,1,1)$	12,14,17,18	6,9,11,17,18	2^{-23}
$(0,0,0,0,0,1,0,0,1,0,1,1,0,1,0,1) \xrightarrow{1r} (0,1,1,1,0,0,1,1,1,0,1,0,1,1,0,1)$	12,14,16	6,9,11	$2^{-28.5}$
$(0,0,0,0,0,1,0,0,1,0,1,1,0,1,1,0) \xrightarrow{1r} (0,1,0,0,1,1,0,1,0,1,0,1,0,0,1,1)$	12,14,17	6,9,11,15,17	2^{-23}
$(0,0,0,0,0,1,0,0,1,0,1,1,0,1,1,1) \xrightarrow{1r} (1,0,1,1,0,0,1,0,1,0,1,0,1,1,0,1)$	12,14,16,18	6,9,11,15,18	$2^{-28.5}$
$(0,0,0,0,0,1,0,0,1,0,1,1,1,0,0,0) \xrightarrow{1r} (1,0,0,0,0,1,0,1,0,1,1,0,1,1,0,0)$	12,18	6,9,11,13,18	2^{-23}
$(0,0,0,0,0,1,0,0,1,0,1,1,1,0,0,1) \xrightarrow{1r} (0,1,1,1,1,0,1,0,1,0,0,1,0,0,1,0)$	12,16,17	6,9,11,13,17	$2^{-28.5}$
$(0,0,0,0,0,1,0,0,1,0,1,1,1,0,1,0) \xrightarrow{1r} (0,1,0,0,0,1,0,0,0,1,1,0,1,1,0,0)$	12	6,9,11,13,15	2^{-23}
$(0,0,0,0,0,1,0,0,1,0,1,1,1,0,1,1) \xrightarrow{1r} (1,0,1,1,1,0,1,1,1,0,0,1,0,0,1,0)$	12,16,17,18	6,9,11,13,15,17,18	$2^{-28.5}$
$(0,0,0,0,0,1,0,0,1,0,1,1,1,1,0,0) \xrightarrow{1r} (0,1,0,1,1,0,0,0,0,0,0,1,0,0,1,1)$	12,14,17	6,9,11,13,17	$2^{-17.5}$
$(0,0,0,0,0,1,0,0,1,0,1,1,1,1,0,1) \xrightarrow{1r} (1,0,1,0,0,1,1,1,1,1,1,0,1,1,0,1)$	12,14,16,18	6,9,11,13,18	2^{-23}
$(0,0,0,0,0,1,0,0,1,0,1,1,1,1,1,0) \xrightarrow{1r} (1,0,0,1,1,0,0,1,0,0,0,1,0,0,1,1)$	12,14,17,18	6,9,11,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,0,0,1,0,1,1,1,1,1,1) \xrightarrow{1r} (0,1,1,0,0,1,1,0,1,1,1,0,1,1,0,1)$	12,14,16	6,9,11,13,15	2^{-23}

Table 0.39 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	10,18	6,9,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	10,16,17	6,9,17	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	10	6,9,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	10,16,17,18	6,9,15,17,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	10,14,17	6,9,17	2^{-1}
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	10,14,16,18	6,9,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	10,14,17,18	6,9,15,17,18	2^{-1}
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	10,14,16	6,9,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	10	6,9,13	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	10,16,17,18	6,9,13,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	10,18	6,9,13,15,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	10,16,17	6,9,13,15,17	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	10,14,17,18	6,9,13,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	10,14,16	6,9,13	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	10,14,17	6,9,13,15,17	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	10,14,16,18	6,9,13,15,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	10,12,17	6,9,17	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	10,12,16,18	6,9,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	10,12,17,18	6,9,15,17,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	10,12,16	6,9,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	10,12,14,18	6,9,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	10,12,14,16,17	6,9,17	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	10,12,14	6,9,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	10,12,14,16,17,18	6,9,15,17,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	10,12,17,18	6,9,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	10,12,16	6,9,13	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	10,12,17	6,9,13,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	10,12,16,18	6,9,13,15,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	10,12,14	6,9,13	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	10,12,14,16,17,18	6,9,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	10,12,14,18	6,9,13,15,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	10,12,14,16,17	6,9,13,15,17	$2^{-17.5}$

Table 0.40 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,0,1,0,0,1,1,1,0,0,0,0,0) \xrightarrow{1r} (0,1,1,1,1,0,1,1,0,0,1,0,0,1,0,0)$	10	6,9,11	$2^{-17.5}$
$(0,0,0,0,0,1,0,0,1,1,1,0,0,0,0,1) \xrightarrow{1r} (1,0,0,0,0,1,0,0,1,1,0,1,1,0,1,0)$	10,16,17,18	6,9,11,17,18	2^{-12}
$(0,0,0,0,0,1,0,0,1,1,1,0,0,0,1,0) \xrightarrow{1r} (1,0,1,1,1,0,1,0,0,0,1,0,0,1,0,0)$	10,18	6,9,11,15,18	$2^{-17.5}$
$(0,0,0,0,0,1,0,0,1,1,1,0,0,0,1,1) \xrightarrow{1r} (0,1,0,0,0,1,0,1,1,1,0,1,1,0,1,0)$	10,16,17	6,9,11,15,17	2^{-12}
$(0,0,0,0,0,1,0,0,1,1,1,0,0,1,0,0) \xrightarrow{1r} (1,0,1,0,0,1,1,0,0,1,0,1,1,0,1,1)$	10,14,17,18	6,9,11,17,18	2^{-12}
$(0,0,0,0,0,1,0,0,1,1,1,0,0,1,0,1) \xrightarrow{1r} (0,1,0,1,1,0,0,1,1,0,1,0,0,1,0,1)$	10,14,16	6,9,11	$2^{-28.5}$
$(0,0,0,0,0,1,0,0,1,1,1,0,0,1,1,0) \xrightarrow{1r} (0,1,1,0,0,1,1,1,0,1,0,1,1,0,1,1)$	10,14,17	6,9,11,15,17	2^{-12}
$(0,0,0,0,0,1,0,0,1,1,1,0,0,1,1,1) \xrightarrow{1r} (1,0,0,1,1,0,0,0,1,0,1,0,0,1,0,1)$	10,14,16,18	6,9,11,15,18	$2^{-28.5}$
$(0,0,0,0,0,1,0,0,1,1,1,0,1,0,0,0) \xrightarrow{1r} (1,0,1,0,1,1,1,1,0,1,1,0,0,1,0,0)$	10,18	6,9,11,13,18	2^{-23}
$(0,0,0,0,0,1,0,0,1,1,1,0,1,0,0,1) \xrightarrow{1r} (0,1,0,1,0,0,0,0,1,0,0,1,1,0,1,0)$	10,16,17	6,9,11,13,17	$2^{-17.5}$
$(0,0,0,0,0,1,0,0,1,1,1,0,1,0,1,0) \xrightarrow{1r} (0,1,1,0,1,1,1,0,0,1,1,0,0,1,0,0)$	10	6,9,11,13,15	2^{-23}
$(0,0,0,0,0,1,0,0,1,1,1,0,1,0,1,1) \xrightarrow{1r} (1,0,0,1,0,0,0,1,1,0,0,1,1,0,1,0)$	10,16,17,18	6,9,11,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,0,0,1,1,1,0,1,1,0,0) \xrightarrow{1r} (0,1,1,1,0,0,1,0,0,0,0,1,1,0,1,1)$	10,14,17	6,9,11,13,17	$2^{-6.5}$
$(0,0,0,0,0,1,0,0,1,1,1,0,1,1,0,1) \xrightarrow{1r} (1,0,0,0,1,1,0,1,1,1,1,0,0,1,0,1)$	10,14,16,18	6,9,11,13,18	2^{-23}
$(0,0,0,0,0,1,0,0,1,1,1,0,1,1,1,0) \xrightarrow{1r} (1,0,1,1,0,0,1,1,0,0,0,1,1,0,1,1)$	10,14,17,18	6,9,11,13,15,17,18	$2^{-6.5}$
$(0,0,0,0,0,1,0,0,1,1,1,0,1,1,1,1) \xrightarrow{1r} (0,1,0,0,1,1,0,0,1,1,1,0,0,1,0,1)$	10,14,16	6,9,11,13,15	2^{-23}
$(0,0,0,0,0,1,0,0,1,1,1,1,0,0,0,0) \xrightarrow{1r} (1,0,1,0,0,1,0,0,0,1,1,1,1,0,1,1)$	10,12,17,18	6,9,11,17,18	2^{-12}
$(0,0,0,0,0,1,0,0,1,1,1,1,0,0,0,1) \xrightarrow{1r} (0,1,0,1,1,0,1,1,1,0,0,0,0,1,0,1)$	10,12,16	6,9,11	$2^{-17.5}$
$(0,0,0,0,0,1,0,0,1,1,1,1,0,0,1,0) \xrightarrow{1r} (0,1,1,0,0,1,0,1,0,1,1,1,1,0,1,1)$	10,12,17	6,9,11,15,17	2^{-12}
$(0,0,0,0,0,1,0,0,1,1,1,1,0,0,1,1) \xrightarrow{1r} (1,0,0,1,1,0,1,0,1,0,0,0,0,1,0,1)$	10,12,16,18	6,9,11,15,18	$2^{-17.5}$
$(0,0,0,0,0,1,0,0,1,1,1,1,0,1,0,0) \xrightarrow{1r} (0,1,1,1,1,0,0,1,0,0,0,0,0,1,0,0)$	10,12,14	6,9,11	$2^{-6.5}$
$(0,0,0,0,0,1,0,0,1,1,1,1,0,1,0,1) \xrightarrow{1r} (1,0,0,0,0,1,1,0,1,1,1,1,1,0,1,0)$	10,12,14,16,17,18	6,9,11,17,18	2^{-12}
$(0,0,0,0,0,1,0,0,1,1,1,1,0,1,1,0) \xrightarrow{1r} (1,0,1,1,1,0,0,0,0,0,0,0,0,1,0,0)$	10,12,14,18	6,9,11,15,18	$2^{-6.5}$
$(0,0,0,0,0,1,0,0,1,1,1,1,0,1,1,1) \xrightarrow{1r} (0,1,0,0,0,1,1,1,1,1,1,1,1,0,1,0)$	10,12,14,16,17	6,9,11,15,17	2^{-12}
$(0,0,0,0,0,1,0,0,1,1,1,1,1,0,0,0) \xrightarrow{1r} (0,1,1,1,0,0,0,0,0,0,0,1,1,1,0,1)$	10,12,17	6,9,11,13,17	$2^{-6.5}$
$(0,0,0,0,0,1,0,0,1,1,1,1,1,0,0,1) \xrightarrow{1r} (1,0,0,0,1,1,1,1,1,1,0,0,0,1,0,1)$	10,12,16,18	6,9,11,13,18	2^{-12}
$(0,0,0,0,0,1,0,0,1,1,1,1,1,0,1,0) \xrightarrow{1r} (1,0,1,1,0,0,0,1,0,0,1,1,1,0,1,1)$	10,12,17,18	6,9,11,13,15,17,18	$2^{-6.5}$
$(0,0,0,0,0,1,0,0,1,1,1,1,1,0,1,1) \xrightarrow{1r} (0,1,0,0,1,1,1,0,1,1,0,0,0,1,0,1)$	10,12,16	6,9,11,13,15	2^{-12}
$(0,0,0,0,0,1,0,0,1,1,1,1,1,1,0,0) \xrightarrow{1r} (1,0,1,0,1,1,0,1,0,1,0,1,0,0,0,0)$	10,12,14,18	6,9,11,13,18	2^{-12}
$(0,0,0,0,0,1,0,0,1,1,1,1,1,1,0,1) \xrightarrow{1r} (0,1,0,1,0,0,1,0,1,0,1,1,1,0,1,0)$	10,12,14,16,17	6,9,11,13,17	$2^{-17.5}$
$(0,0,0,0,0,1,0,0,1,1,1,1,1,1,1,0) \xrightarrow{1r} (0,1,1,0,1,1,0,0,0,1,0,0,0,1,0,0)$	10,12,14	6,9,11,13,15	2^{-12}
$(0,0,0,0,0,1,0,0,1,1,1,1,1,1,1,1) \xrightarrow{1r} (1,0,0,1,0,0,1,1,1,0,1,1,1,0,1,0)$	10,12,14,16,17,18	6,9,11,13,15,17,18	$2^{-17.5}$

Table 0.41 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	—	6,8	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	16,17,18	6,8,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	18	6,8,15,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	16,17	6,8,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	14,17,18	6,8,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	14,16	6,8	2^{-1}
$(0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	14,17	6,8,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	14,16,18	6,8,15,18	2^{-1}
$(0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	18	6,8,13,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	16,17	6,8,13,17	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	—	6,8,13,15	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	16,17,18	6,8,13,15,17,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	14,17	6,8,13,17	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	14,16,18	6,8,13,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	14,17,18	6,8,13,15,17,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	14,16	6,8,13,15	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	12,17,18	6,8,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	12,16	6,8	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	12,17	6,8,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	12,16,18	6,8,15,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	12,14	6,8	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	12,14,16,17,18	6,8,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	12,14,18	6,8,15,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	12,14,16,17	6,8,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	12,17	6,8,13,17	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	12,16,18	6,8,13,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	12,17,18	6,8,13,15,17,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	12,16	6,8,13,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	12,14,18	6,8,13,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	12,14,16,17	6,8,13,17	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	12,14	6,8,13,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	12,14,16,17,18	6,8,13,15,17,18	2^{-12}

Table 0.42 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,0,1,0,1,0,0,1,0,0,0,0,0) \xrightarrow{1r} (1,1,1,0,0,1,0,0,1,1,0,1,1,0,1,0)$	18	6,8,11,18	2^{-12}
$(0,0,0,0,0,1,0,1,0,0,1,0,0,0,0,1) \xrightarrow{1r} (0,0,0,1,1,0,1,1,0,0,1,0,0,1,0,0)$	16,17	6,8,11,17	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,0,0,1,0,0,0,1,0) \xrightarrow{1r} (0,0,1,0,0,1,0,1,1,1,0,1,1,0,1,0)$	—	6,8,11,15	2^{-12}
$(0,0,0,0,0,1,0,1,0,0,1,0,0,0,1,1) \xrightarrow{1r} (1,1,0,1,1,0,1,0,0,0,1,0,0,1,0,0)$	16,17,18	6,8,11,15,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,0,0,1,0,0,1,0,0) \xrightarrow{1r} (0,0,1,1,1,0,0,1,1,0,1,0,0,1,0,1)$	14,17	6,8,11,17	$2^{-28.5}$
$(0,0,0,0,0,1,0,1,0,0,1,0,0,1,0,1) \xrightarrow{1r} (1,1,0,0,0,1,1,0,0,1,0,1,1,0,1,1)$	14,16,18	6,8,11,18	2^{-12}
$(0,0,0,0,0,1,0,1,0,0,1,0,0,1,1,0) \xrightarrow{1r} (1,1,1,1,1,0,0,0,1,0,1,0,0,1,0,1)$	14,17,18	6,8,11,15,17,18	$2^{-28.5}$
$(0,0,0,0,0,1,0,1,0,0,1,0,0,1,1,1) \xrightarrow{1r} (0,0,0,0,0,1,1,1,0,1,0,1,1,0,1,1)$	14,16	6,8,11,15	2^{-12}
$(0,0,0,0,0,1,0,1,0,0,1,0,1,0,0,0) \xrightarrow{1r} (0,0,1,1,0,0,0,0,1,0,0,1,1,0,1,0)$	—	6,8,11,13	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,0,0,1,0,1,0,0,1) \xrightarrow{1r} (1,1,0,0,1,1,1,1,0,1,1,0,0,1,0,0)$	16,17,18	6,8,11,13,17,18	2^{-23}
$(0,0,0,0,0,1,0,1,0,0,1,0,1,0,1,0) \xrightarrow{1r} (1,1,1,1,0,0,0,1,1,0,0,1,1,0,1,0)$	18	6,8,11,13,15,18	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,0,0,1,0,1,0,1,1) \xrightarrow{1r} (0,0,0,0,1,1,1,0,0,1,1,0,0,1,0,0)$	16,17	6,8,11,13,15,17	2^{-23}
$(0,0,0,0,0,1,0,1,0,0,1,0,1,1,0,0) \xrightarrow{1r} (1,1,1,0,1,1,0,1,1,1,1,0,0,1,0,1)$	14,17,18	6,8,11,13,17,18	2^{-23}
$(0,0,0,0,0,1,0,1,0,0,1,0,1,1,0,1) \xrightarrow{1r} (0,0,0,1,0,0,1,0,0,0,0,1,1,0,1,1)$	14,16	6,8,11,13	$2^{-6.5}$
$(0,0,0,0,0,1,0,1,0,0,1,0,1,1,1,0) \xrightarrow{1r} (0,0,1,0,1,1,0,0,1,1,1,0,0,1,0,1)$	14,17	6,8,11,13,15,17	2^{-23}
$(0,0,0,0,0,1,0,1,0,0,1,0,1,1,1,1) \xrightarrow{1r} (1,1,0,1,0,0,1,1,0,0,0,1,1,0,1,1)$	14,16,18	6,8,11,13,15,18	$2^{-6.5}$
$(0,0,0,0,0,1,0,1,0,0,1,1,0,0,0,0) \xrightarrow{1r} (0,0,1,1,1,0,1,1,1,0,0,0,0,1,0,1)$	12,17	6,8,11,17	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,0,0,1,1,0,0,0,1) \xrightarrow{1r} (1,1,0,0,0,1,0,0,0,1,1,1,1,0,1,1)$	12,16,18	6,8,11,18	2^{-12}
$(0,0,0,0,0,1,0,1,0,0,1,1,0,0,1,0) \xrightarrow{1r} (1,1,1,1,1,0,1,0,1,0,0,0,0,1,0,1)$	12,17,18	6,8,11,15,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,0,0,1,1,0,0,1,1) \xrightarrow{1r} (0,0,0,0,0,1,0,1,0,1,1,1,1,0,1,1)$	12,16	6,8,11,15	2^{-12}
$(0,0,0,0,0,1,0,1,0,0,1,1,0,1,0,0) \xrightarrow{1r} (1,1,1,0,0,1,1,0,1,1,1,1,1,0,1,0)$	12,14,18	6,8,11,18	2^{-12}
$(0,0,0,0,0,1,0,1,0,0,1,1,0,1,0,1) \xrightarrow{1r} (0,0,0,1,1,0,0,1,0,0,0,0,0,1,0,0)$	12,14,16,17	6,8,11,17	$2^{-6.5}$
$(0,0,0,0,0,1,0,1,0,0,1,1,0,1,1,0) \xrightarrow{1r} (0,0,1,0,0,1,1,1,1,1,1,1,1,0,1,0)$	12,14	6,8,11,15	2^{-12}
$(0,0,0,0,0,1,0,1,0,0,1,1,0,1,1,1) \xrightarrow{1r} (1,1,0,1,1,0,0,0,0,0,0,0,0,0,1,0)$	12,14,16,17,18	6,8,11,15,17,18	$2^{-6.5}$
$(0,0,0,0,0,1,0,1,0,0,1,1,1,0,0,0) \xrightarrow{1r} (1,1,1,0,1,1,1,1,1,1,0,0,0,1,0,1)$	12,17,18	6,8,11,13,17,18	2^{-12}
$(0,0,0,0,0,1,0,1,0,0,1,1,1,0,0,1) \xrightarrow{1r} (0,0,0,1,0,0,0,0,0,0,0,1,1,1,0,1)$	12,16	6,8,11,13	$2^{-6.5}$
$(0,0,0,0,0,1,0,1,0,0,1,1,1,0,1,0) \xrightarrow{1r} (0,0,1,0,1,1,1,0,1,1,0,0,0,1,0,1)$	12,17	6,8,11,13,15,17	2^{-12}
$(0,0,0,0,0,1,0,1,0,0,1,1,1,0,1,1) \xrightarrow{1r} (1,1,0,1,0,0,0,1,0,0,1,1,1,0,1,1)$	12,16,18	6,8,11,13,15,18	$2^{-6.5}$
$(0,0,0,0,0,1,0,1,0,0,1,1,1,1,0,0) \xrightarrow{1r} (0,0,1,1,0,0,1,0,1,0,1,1,1,0,1,0)$	12,14	6,8,11,13	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,0,0,1,1,1,1,0,1) \xrightarrow{1r} (1,1,0,0,1,1,0,1,0,1,0,0,0,1,0,0)$	12,14,16,17,18	6,8,11,13,17,18	2^{-12}
$(0,0,0,0,0,1,0,1,0,0,1,1,1,1,1,0) \xrightarrow{1r} (1,1,1,1,0,0,1,1,1,0,1,1,1,0,1,0)$	12,14,18	6,8,11,13,15,18	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,0,0,1,1,1,1,1,1) \xrightarrow{1r} (0,0,0,0,1,1,0,0,0,1,0,0,0,1,0,0)$	12,14,16,17	6,8,11,13,15,17	2^{-12}

Table 0.43 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,0,1,0,1,0,1,0,0,0,0,0,0) \xrightarrow{1r} (1,1,0,1,0,1,0,1,1,1,0,1,1,1,0,1)$	10,17,18	6,8,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,0,1,0,0,0,0,0,1) \xrightarrow{1r} (0,0,1,0,1,0,1,0,0,0,1,0,0,0,1,1)$	10,16	6,8	2^{-23}
$(0,0,0,0,0,1,0,1,0,1,0,0,0,0,1,0) \xrightarrow{1r} (0,0,0,1,0,1,0,0,1,1,0,1,1,1,0,1)$	10,17	6,8,15,17	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,0,1,0,0,0,0,1,1) \xrightarrow{1r} (1,1,1,0,1,0,1,1,0,0,1,0,0,0,1,1)$	10,16,18	6,8,15,18	2^{-23}
$(0,0,0,0,0,1,0,1,0,1,0,0,0,1,0,0) \xrightarrow{1r} (0,0,0,0,1,0,0,0,1,0,1,0,0,0,1,0)$	10,14	6,8	2^{-34}
$(0,0,0,0,0,1,0,1,0,1,0,0,0,1,0,1) \xrightarrow{1r} (1,1,1,1,0,1,1,1,0,1,0,1,1,1,0,0)$	10,14,16,17,18	6,8,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,0,1,0,0,0,1,1,0) \xrightarrow{1r} (1,1,0,0,1,0,0,1,1,0,1,0,0,0,1,0)$	10,14,18	6,8,15,18	2^{-34}
$(0,0,0,0,0,1,0,1,0,1,0,0,0,1,1,1) \xrightarrow{1r} (0,0,1,1,0,1,1,0,0,1,0,1,1,1,0,0)$	10,14,16,17	6,8,15,17	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,0,1,0,0,1,0,0,0) \xrightarrow{1r} (0,0,0,0,0,0,0,1,1,0,0,1,1,1,0,1)$	10,17	6,8,13,17	2^{-23}
$(0,0,0,0,0,1,0,1,0,1,0,0,1,0,0,1) \xrightarrow{1r} (1,1,1,1,1,1,0,0,1,1,0,0,0,1,1,1)$	10,16,18	6,8,13,18	$2^{-28.5}$
$(0,0,0,0,0,1,0,1,0,1,0,0,1,0,1,0) \xrightarrow{1r} (1,1,0,0,0,0,0,0,1,0,0,1,1,1,0,1)$	10,17,18	6,8,13,15,17,18	2^{-23}
$(0,0,0,0,0,1,0,1,0,1,0,0,1,0,1,1) \xrightarrow{1r} (0,0,1,1,1,1,1,1,0,1,1,0,0,0,1,1)$	10,16	6,8,13,15	$2^{-28.5}$
$(0,0,0,0,0,1,0,1,0,1,0,0,1,1,0,0) \xrightarrow{1r} (1,1,0,1,1,1,0,0,1,1,1,0,0,0,1,0)$	10,14,18	6,8,13,18	$2^{-28.5}$
$(0,0,0,0,0,1,0,1,0,1,0,0,1,1,0,1) \xrightarrow{1r} (0,0,1,0,0,0,1,1,0,0,0,1,1,1,0,0)$	10,14,16,17	6,8,13,17	2^{-12}
$(0,0,0,0,0,1,0,1,0,1,0,0,1,1,1,0) \xrightarrow{1r} (0,0,0,1,1,1,0,1,1,1,1,0,0,0,1,0)$	10,14	6,8,13,15	$2^{-28.5}$
$(0,0,0,0,0,1,0,1,0,1,0,0,1,1,1,1) \xrightarrow{1r} (1,1,1,0,0,0,1,0,0,0,0,1,1,1,0,0)$	10,14,16,17,18	6,8,13,15,17,18	2^{-12}
$(0,0,0,0,0,1,0,1,0,1,0,1,0,0,0,0) \xrightarrow{1r} (0,0,0,0,1,0,1,0,1,0,0,0,0,0,1,0)$	10,12	6,8	2^{-23}
$(0,0,0,0,0,1,0,1,0,1,0,1,0,0,0,1) \xrightarrow{1r} (1,1,1,1,0,1,0,1,0,1,1,1,1,1,0,0)$	10,12,16,17,18	6,8,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,0,1,0,1,0,0,1,0) \xrightarrow{1r} (1,1,0,0,1,0,1,1,1,0,0,0,0,0,1,0)$	10,12,18	6,8,15,18	2^{-23}
$(0,0,0,0,0,1,0,1,0,1,0,1,0,0,1,1) \xrightarrow{1r} (0,0,1,1,0,1,0,0,0,1,1,1,1,1,0,0)$	10,12,16,17	6,8,15,17	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,0,1,0,1,0,1,0,0) \xrightarrow{1r} (1,1,0,1,0,1,1,1,1,1,1,1,1,1,0,1)$	10,12,14,17,18	6,8,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,0,1,0,1,0,1,0,1) \xrightarrow{1r} (0,0,1,0,1,0,0,0,0,0,0,0,0,0,1,1)$	10,12,14,16	6,8	2^{-12}
$(0,0,0,0,0,1,0,1,0,1,0,1,0,1,1,0) \xrightarrow{1r} (0,0,0,1,0,1,1,0,1,1,1,1,1,1,0,1)$	10,12,14,17	6,8,15,17	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,0,1,0,1,0,1,1,1) \xrightarrow{1r} (1,1,1,0,1,0,0,1,0,0,0,0,0,0,1,1)$	10,12,14,16,18	6,8,15,18	2^{-12}
$(0,0,0,0,0,1,0,1,0,1,0,1,1,0,0,0) \xrightarrow{1r} (1,1,0,1,1,1,1,0,1,1,0,0,0,0,1,0)$	10,12,18	6,8,13,18	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,0,1,0,1,1,0,0,1) \xrightarrow{1r} (0,0,1,0,0,0,0,1,0,0,1,1,1,1,0,0)$	10,12,16,17	6,8,13,17	2^{-12}
$(0,0,0,0,0,1,0,1,0,1,0,1,1,0,1,0) \xrightarrow{1r} (0,0,0,1,1,1,1,1,1,1,0,0,0,0,1,0)$	10,12	6,8,13,15	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,0,1,0,1,1,0,1,1) \xrightarrow{1r} (1,1,1,0,0,0,0,0,0,0,1,1,1,1,0,0)$	10,12,16,17,18	6,8,13,15,17,18	2^{-12}
$(0,0,0,0,0,1,0,1,0,1,0,1,1,1,0,0) \xrightarrow{1r} (0,0,0,0,0,0,1,1,1,0,1,1,1,1,0,1)$	10,12,14,17	6,8,13,17	2^{-23}
$(0,0,0,0,0,1,0,1,0,1,0,1,1,1,0,1) \xrightarrow{1r} (1,1,1,1,1,1,0,0,0,1,0,0,0,0,1,1)$	10,12,14,16,18	6,8,13,18	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,0,1,0,1,1,1,1,0) \xrightarrow{1r} (1,1,0,0,0,0,1,0,1,0,1,1,1,1,0,1)$	10,12,14,17,18	6,8,13,15,17,18	2^{-23}
$(0,0,0,0,0,1,0,1,0,1,0,1,1,1,1,1) \xrightarrow{1r} (0,0,1,1,1,1,0,1,0,1,0,0,0,0,1,1)$	10,12,14,16	6,8,13,15	$2^{-17.5}$

Table 0.44 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,0,1,0,1,0,1,1,0,0,0,0,0) \xrightarrow{1r} (0,0,0,1,0,0,0,1,1,0,0,0,1,1,0,1)$	10,17	6,8,11,17	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,0,1,1,0,0,0,0,1) \xrightarrow{1r} (1,1,1,0,1,1,1,0,0,1,1,1,0,0,1,1)$	10,16,18	6,8,11,18	2^{-23}
$(0,0,0,0,0,1,0,1,0,1,1,0,0,0,1,0) \xrightarrow{1r} (1,1,0,1,0,0,0,0,1,0,0,0,1,1,0,1)$	10,17,18	6,8,11,15,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,0,1,1,0,0,0,1,1) \xrightarrow{1r} (0,0,1,0,1,1,1,1,0,1,1,1,0,0,1,1)$	10,16	6,8,11,15	2^{-23}
$(0,0,0,0,0,1,0,1,0,1,1,0,0,1,0,0) \xrightarrow{1r} (1,1,0,0,1,1,0,0,1,1,1,1,0,0,1,0)$	10,14,18	6,8,11,18	2^{-23}
$(0,0,0,0,0,1,0,1,0,1,1,0,0,1,0,1) \xrightarrow{1r} (0,0,1,1,0,0,1,1,0,0,0,0,1,1,0,0)$	10,14,16,17	6,8,11,17	$2^{-6.5}$
$(0,0,0,0,0,1,0,1,0,1,1,0,0,1,1,0) \xrightarrow{1r} (0,0,0,0,1,1,0,1,1,1,1,1,0,0,1,0)$	10,14	6,8,11,15	2^{-23}
$(0,0,0,0,0,1,0,1,0,1,1,0,0,1,1,1) \xrightarrow{1r} (1,1,1,1,0,0,1,0,0,0,0,0,1,1,0,0)$	10,14,16,17,18	6,8,11,15,17,18	$2^{-6.5}$
$(0,0,0,0,0,1,0,1,0,1,1,0,1,0,0,0) \xrightarrow{1r} (1,1,0,0,0,1,0,1,1,1,0,0,1,1,0,1)$	10,17,18	6,8,11,13,17,18	2^{-12}
$(0,0,0,0,0,1,0,1,0,1,1,0,1,0,0,1) \xrightarrow{1r} (0,0,1,1,1,0,1,0,0,0,1,1,0,0,1,1)$	10,16	6,8,11,13	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,0,1,1,0,1,0,1,0) \xrightarrow{1r} (0,0,0,0,0,1,0,0,1,1,0,0,1,1,0,1)$	10,17	6,8,11,13,15,17	2^{-12}
$(0,0,0,0,0,1,0,1,0,1,1,0,1,0,1,1) \xrightarrow{1r} (1,1,1,1,1,0,1,1,0,0,1,1,0,0,1,1)$	10,16,18	6,8,11,13,15,18	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,0,1,1,0,1,1,0,0) \xrightarrow{1r} (0,0,0,1,1,0,0,0,1,0,1,1,0,0,1,0)$	10,14	6,8,11,13	$2^{-28.5}$
$(0,0,0,0,0,1,0,1,0,1,1,0,1,1,0,1) \xrightarrow{1r} (1,1,1,0,0,1,1,1,0,1,0,0,1,1,0,0)$	10,14,16,17,18	6,8,11,13,17,18	2^{-12}
$(0,0,0,0,0,1,0,1,0,1,1,0,1,1,1,0) \xrightarrow{1r} (1,1,0,1,1,0,0,1,1,0,1,1,0,0,1,0)$	10,14,18	6,8,11,13,15,18	$2^{-28.5}$
$(0,0,0,0,0,1,0,1,0,1,1,0,1,1,1,1) \xrightarrow{1r} (0,0,1,0,0,1,1,0,0,1,0,0,1,1,0,0)$	10,14,16,17	6,8,11,13,15,17	2^{-12}
$(0,0,0,0,0,1,0,1,0,1,1,1,0,0,0,0) \xrightarrow{1r} (1,1,0,0,1,1,1,0,1,1,0,1,0,0,1,0)$	10,12,18	6,8,11,18	2^{-23}
$(0,0,0,0,0,1,0,1,0,1,1,1,0,0,0,1) \xrightarrow{1r} (0,0,1,1,0,0,0,1,0,0,1,0,1,1,0,0)$	10,12,16,17	6,8,11,17	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,0,1,1,1,0,0,1,0) \xrightarrow{1r} (0,0,0,0,1,1,1,1,1,1,0,1,0,0,1,0)$	10,12	6,8,11,15	2^{-23}
$(0,0,0,0,0,1,0,1,0,1,1,1,0,0,1,1) \xrightarrow{1r} (1,1,1,1,0,0,0,0,0,0,1,0,1,1,0,0)$	10,12,16,17,18	6,8,11,15,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,0,1,1,1,0,1,0,0) \xrightarrow{1r} (0,0,0,1,0,0,1,1,1,0,1,0,1,1,0,1)$	10,12,14,17	6,8,11,17	$2^{-28.5}$
$(0,0,0,0,0,1,0,1,0,1,1,1,0,1,0,1) \xrightarrow{1r} (1,1,1,0,1,1,0,0,0,1,0,1,0,0,1,1)$	10,12,14,16,18	6,8,11,18	2^{-23}
$(0,0,0,0,0,1,0,1,0,1,1,1,0,1,1,0) \xrightarrow{1r} (1,1,0,1,0,0,1,0,1,0,1,0,1,0,1,1)$	10,12,14,17,18	6,8,11,15,17,18	$2^{-28.5}$
$(0,0,0,0,0,1,0,1,0,1,1,1,0,1,1,1) \xrightarrow{1r} (0,0,1,0,1,1,0,1,0,1,0,1,0,0,1,1)$	10,12,14,16	6,8,11,15	2^{-23}
$(0,0,0,0,0,1,0,1,0,1,1,1,1,0,0,0) \xrightarrow{1r} (0,0,0,1,1,0,1,0,1,0,1,0,0,1,0,0)$	10,12	6,8,11,13	$2^{-28.5}$
$(0,0,0,0,0,1,0,1,0,1,1,1,1,0,0,1) \xrightarrow{1r} (1,1,1,0,0,1,0,1,0,1,0,1,1,0,1,0)$	10,12,16,17,18	6,8,11,13,17,18	2^{-23}
$(0,0,0,0,0,1,0,1,0,1,1,1,1,0,1,0) \xrightarrow{1r} (1,1,0,1,1,0,1,1,1,0,0,1,0,0,1,0)$	10,12,18	6,8,11,13,15,18	$2^{-28.5}$
$(0,0,0,0,0,1,0,1,0,1,1,1,1,0,1,1) \xrightarrow{1r} (0,0,1,0,0,1,0,0,0,1,1,0,1,1,0,0)$	10,12,16,17	6,8,11,13,15,17	2^{-23}
$(0,0,0,0,0,1,0,1,0,1,1,1,1,1,0,0) \xrightarrow{1r} (1,1,0,0,0,1,1,1,1,1,1,0,1,0,1,1)$	10,12,14,17,18	6,8,11,13,17,18	2^{-23}
$(0,0,0,0,0,1,0,1,0,1,1,1,1,1,0,1) \xrightarrow{1r} (0,0,1,1,1,0,0,0,0,0,0,1,0,0,1,1)$	10,12,14,16	6,8,11,13	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,0,1,1,1,1,1,1,0) \xrightarrow{1r} (0,0,0,0,0,1,1,0,1,1,1,0,1,1,0,1)$	10,12,14,17	6,8,11,13,15,17	2^{-23}
$(0,0,0,0,0,1,0,1,0,1,1,1,1,1,1,1) \xrightarrow{1r} (1,1,1,1,1,0,0,1,0,0,0,1,0,0,1,1)$	10,12,14,16,18	6,8,11,13,15,18	$2^{-17.5}$

Table 0.45 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,0,1,0,1,1,0,0,0,0,0,0,0) \xrightarrow{1r} (1,0,1,1,0,1,0,1,1,1,0,1,1,1,1,0)$	18	6,8,9,18	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,1,0,0,0,0,0,0,1) \xrightarrow{1r} (0,1,0,0,1,0,1,0,0,0,1,0,0,0,0,0)$	16,17	6,8,9,17	2^{-23}
$(0,0,0,0,0,1,0,1,1,0,0,0,0,0,1,0) \xrightarrow{1r} (0,1,1,1,0,1,0,0,1,1,0,1,1,1,1,0)$	—	6,8,9,15	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,1,0,0,0,0,0,1,1) \xrightarrow{1r} (1,0,0,0,1,0,1,1,0,0,1,0,0,0,0,0)$	16,17,18	6,8,9,15,17,18	2^{-23}
$(0,0,0,0,0,1,0,1,1,0,0,0,0,1,0,0) \xrightarrow{1r} (0,1,1,0,1,0,0,0,1,0,1,0,0,0,0,1)$	14,17	6,8,9,17	2^{-34}
$(0,0,0,0,0,1,0,1,1,0,0,0,0,1,0,1) \xrightarrow{1r} (1,0,0,1,0,1,1,1,0,1,0,1,1,1,1,1)$	14,16,18	6,8,9,18	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,1,0,0,0,0,1,1,0) \xrightarrow{1r} (1,0,1,0,1,0,0,1,1,0,1,0,0,0,0,1)$	14,17,18	6,8,9,15,17,18	2^{-34}
$(0,0,0,0,0,1,0,1,1,0,0,0,0,1,1,1) \xrightarrow{1r} (0,1,0,1,0,1,1,0,0,1,0,1,1,1,1,1)$	14,16	6,8,9,15	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,1,0,0,0,1,0,0,0) \xrightarrow{1r} (0,1,1,0,0,0,0,1,1,0,0,1,1,1,1,0)$	—	6,8,9,13	2^{-23}
$(0,0,0,0,0,1,0,1,1,0,0,0,1,0,0,1) \xrightarrow{1r} (1,0,0,1,1,1,1,0,0,1,1,0,0,0,0,0)$	16,17,18	6,8,9,13,17,18	$2^{-28.5}$
$(0,0,0,0,0,1,0,1,1,0,0,0,1,0,1,0) \xrightarrow{1r} (1,0,1,0,0,0,0,0,1,0,0,1,1,1,1,0)$	18	6,8,9,13,15,18	2^{-23}
$(0,0,0,0,0,1,0,1,1,0,0,0,1,0,1,1) \xrightarrow{1r} (0,1,0,1,1,1,1,1,0,1,1,0,0,0,0,0)$	16,17	6,8,9,13,15,17	$2^{-28.5}$
$(0,0,0,0,0,1,0,1,1,0,0,0,1,1,0,0) \xrightarrow{1r} (1,0,1,1,1,1,0,0,1,1,1,0,0,0,0,1)$	14,17,18	6,8,9,13,17,18	$2^{-28.5}$
$(0,0,0,0,0,1,0,1,1,0,0,0,1,1,1,0) \xrightarrow{1r} (0,1,0,0,0,0,1,1,0,0,0,1,1,1,1,1)$	14,16	6,8,9,13	2^{-12}
$(0,0,0,0,0,1,0,1,1,0,0,0,1,1,1,0) \xrightarrow{1r} (0,1,1,1,1,1,0,1,1,1,1,0,0,0,0,1)$	14,17	6,8,9,13,15,17	$2^{-28.5}$
$(0,0,0,0,0,1,0,1,1,0,0,0,1,1,1,1) \xrightarrow{1r} (1,0,0,0,0,0,1,0,0,0,0,1,1,1,1,1)$	14,16,18	6,8,9,13,15,18	2^{-12}
$(0,0,0,0,0,1,0,1,1,0,0,1,0,0,0,0) \xrightarrow{1r} (0,1,1,0,1,0,1,0,1,0,0,0,0,0,0,1)$	12,17	6,8,9,17	2^{-23}
$(0,0,0,0,0,1,0,1,1,0,0,1,0,0,0,1) \xrightarrow{1r} (1,0,0,1,0,1,0,1,0,1,1,1,1,1,1,1)$	12,16,18	6,8,9,18	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,1,0,0,1,0,0,1,0) \xrightarrow{1r} (1,0,1,0,1,0,1,1,1,0,0,0,0,0,0,1)$	12,17,18	6,8,9,15,17,18	2^{-23}
$(0,0,0,0,0,1,0,1,1,0,0,1,0,0,1,1) \xrightarrow{1r} (0,1,0,1,0,1,0,0,0,1,1,1,1,1,1,1)$	12,16	6,8,9,15	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,1,0,0,1,0,1,0,0) \xrightarrow{1r} (1,0,1,1,0,1,1,1,1,1,1,1,1,1,1,0)$	12,14,18	6,8,9,18	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,1,0,0,1,0,1,0,1) \xrightarrow{1r} (0,1,0,0,1,0,0,0,0,0,0,0,0,0,0,0)$	12,14,16,17	6,8,9,17	2^{-12}
$(0,0,0,0,0,1,0,1,1,0,0,1,0,1,1,0) \xrightarrow{1r} (0,1,1,1,0,1,1,0,1,1,1,1,1,1,1,0)$	12,14	6,8,9,15	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,1,0,0,1,0,1,1,1) \xrightarrow{1r} (1,0,0,0,1,0,0,1,0,0,0,0,0,0,0,0)$	12,14,16,17,18	6,8,9,15,17,18	2^{-12}
$(0,0,0,0,0,1,0,1,1,0,0,1,1,0,0,0) \xrightarrow{1r} (1,0,1,1,1,1,1,0,1,1,0,0,0,0,0,1)$	12,17,18	6,8,9,13,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,1,0,0,1,1,0,0,1) \xrightarrow{1r} (0,1,0,0,0,0,0,1,0,0,1,1,1,1,1,1)$	12,16	6,8,9,13	2^{-12}
$(0,0,0,0,0,1,0,1,1,0,0,1,1,0,1,0) \xrightarrow{1r} (0,1,1,1,1,1,1,1,1,1,0,0,0,0,0,1)$	12,17	6,8,9,13,15,17	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,1,0,0,1,1,0,1,1) \xrightarrow{1r} (1,0,0,0,0,0,0,0,0,0,1,1,1,1,1,1)$	12,16,18	6,8,9,13,15,18	2^{-12}
$(0,0,0,0,0,1,0,1,1,0,0,1,1,1,0,0) \xrightarrow{1r} (0,1,1,0,0,0,1,1,1,0,1,1,1,1,1,0)$	12,14	6,8,9,13	2^{-23}
$(0,0,0,0,0,1,0,1,1,0,0,1,1,1,0,1) \xrightarrow{1r} (1,0,0,1,1,1,0,0,0,1,0,0,0,0,0,0)$	12,14,16,17,18	6,8,9,13,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,1,0,0,1,1,1,1,0) \xrightarrow{1r} (1,0,1,0,0,0,1,0,1,0,1,1,1,1,1,0)$	12,14,18	6,8,9,13,15,18	2^{-23}
$(0,0,0,0,0,1,0,1,1,0,0,1,1,1,1,1) \xrightarrow{1r} (0,1,0,1,1,1,0,1,0,1,0,1,0,0,0,0)$	12,14,16,17	6,8,9,13,15,17	$2^{-17.5}$

Table 0.46 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	—	6,8,9,11	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	16,17,18	6,8,9,11,17,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	18	6,8,9,11,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	16,17	6,8,9,11,15,17	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	14,17,18	6,8,9,11,17,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	14,16	6,8,9,11	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	14,17	6,8,9,11,15,17	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	14,16,18	6,8,9,11,15,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	18	6,8,9,11,13,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	16,17	6,8,9,11,13,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	—	6,8,9,11,13,15	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	16,17,18	6,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	14,17	6,8,9,11,13,17	$2^{-28.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	14,16,18	6,8,9,11,13,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	14,17,18	6,8,9,11,13,15,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	14,16	6,8,9,11,13,15	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	12,17,18	6,8,9,11,17,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	12,16	6,8,9,11	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	12,17	6,8,9,11,15,17	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	12,16,18	6,8,9,11,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	12,14	6,8,9,11	$2^{-28.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	12,14,16,17,18	6,8,9,11,17,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	12,14,18	6,8,9,11,15,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	12,14,16,17	6,8,9,11,15,17	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	12,17	6,8,9,11,13,17	$2^{-28.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	12,16,18	6,8,9,11,13,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	12,17,18	6,8,9,11,13,15,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	12,16	6,8,9,11,13,15	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	12,14,18	6,8,9,11,13,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	12,14,16,17	6,8,9,11,13,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	12,14	6,8,9,11,13,15	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	12,14,16,17,18	6,8,9,11,13,15,17,18	$2^{-17.5}$

Table 0.47 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	10,17	6,8,9,17	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	10,16,18	6,8,9,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	10,17,18	6,8,9,15,17,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	10,16	6,8,9,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	10,14,18	6,8,9,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	10,14,16,17	6,8,9,17	2^{-1}
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	10,14	6,8,9,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	10,14,16,17,18	6,8,9,15,17,18	2^{-1}
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	10,17,18	6,8,9,13,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	10,16	6,8,9,13	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	10,17	6,8,9,13,15,17	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	10,16,18	6,8,9,13,15,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	10,14	6,8,9,13	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	10,14,16,17,18	6,8,9,13,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	10,14,18	6,8,9,13,15,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	10,14,16,17	6,8,9,13,15,17	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	10,12,18	6,8,9,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	10,12,16,17	6,8,9,17	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	10,12	6,8,9,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	10,12,16,17,18	6,8,9,15,17,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	10,12,14,17	6,8,9,17	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	10,12,14,16,18	6,8,9,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	10,12,14,17,18	6,8,9,15,17,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	10,12,14,16	6,8,9,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	10,12	6,8,9,13	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	10,12,16,17,18	6,8,9,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	10,12,18	6,8,9,13,15,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	10,12,16,17	6,8,9,13,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	10,12,14,17,18	6,8,9,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	10,12,14,16	6,8,9,13	2^{-12}
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	10,12,14,17	6,8,9,13,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	10,12,14,16,18	6,8,9,13,15,18	2^{-12}

Table 0.48 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,0,1,0,1,1,1,1,0,0,0,0,0) \xrightarrow{1r} (1,0,0,0,0,1,0,0,1,1,0,1,1,0,0,1)$	10,17,18	6,8,9,11,17,18	2^{-12}
$(0,0,0,0,0,1,0,1,1,1,1,0,0,0,0,1) \xrightarrow{1r} (0,1,1,1,1,0,1,1,0,0,1,0,0,1,1,1)$	10,16	6,8,9,11	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,1,1,1,0,0,0,1,0) \xrightarrow{1r} (0,1,0,0,0,1,0,1,1,1,0,1,1,0,0,1)$	10,17	6,8,9,11,15,17	2^{-12}
$(0,0,0,0,0,1,0,1,1,1,1,0,0,0,1,1) \xrightarrow{1r} (1,0,1,1,1,0,1,0,0,0,1,0,0,1,1,1)$	10,16,18	6,8,9,11,15,18	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,1,1,1,0,0,1,0,0) \xrightarrow{1r} (0,1,0,1,1,0,0,1,1,0,1,0,0,1,1,0)$	10,14	6,8,9,11	$2^{-28.5}$
$(0,0,0,0,0,1,0,1,1,1,1,0,0,1,0,1) \xrightarrow{1r} (1,0,1,0,0,1,1,0,0,1,0,1,1,0,0,0)$	10,14,16,17,18	6,8,9,11,17,18	2^{-12}
$(0,0,0,0,0,1,0,1,1,1,1,0,0,1,1,0) \xrightarrow{1r} (1,0,0,1,1,0,0,0,1,0,1,0,0,1,1,0)$	10,14,18	6,8,9,11,15,18	$2^{-28.5}$
$(0,0,0,0,0,1,0,1,1,1,1,0,0,1,1,1) \xrightarrow{1r} (0,1,1,0,0,1,1,1,0,1,0,1,1,0,0,0)$	10,14,16,17	6,8,9,11,15,17	2^{-12}
$(0,0,0,0,0,1,0,1,1,1,1,0,1,0,0,0) \xrightarrow{1r} (0,1,0,1,0,0,0,0,1,0,0,1,1,0,0,1)$	10,17	6,8,9,11,13,17	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,1,1,1,0,1,0,0,1) \xrightarrow{1r} (1,0,1,0,1,1,1,1,0,1,1,0,0,1,1,1)$	10,16,18	6,8,9,11,13,18	2^{-23}
$(0,0,0,0,0,1,0,1,1,1,1,0,1,0,1,0) \xrightarrow{1r} (1,0,0,1,0,0,0,1,1,0,0,1,1,0,0,1)$	10,17,18	6,8,9,11,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,1,1,1,0,1,0,1,1) \xrightarrow{1r} (0,1,1,0,1,1,1,1,0,0,1,1,0,0,1,1,1)$	10,16	6,8,9,11,13,15	2^{-23}
$(0,0,0,0,0,1,0,1,1,1,1,0,1,1,0,0) \xrightarrow{1r} (1,0,0,0,1,1,0,1,1,1,1,0,0,1,1,0)$	10,14,18	6,8,9,11,13,18	2^{-23}
$(0,0,0,0,0,1,0,1,1,1,1,0,1,1,0,1) \xrightarrow{1r} (0,1,1,1,0,0,1,0,0,0,0,1,1,0,0,0)$	10,14,16,17	6,8,9,11,13,17	$2^{-6.5}$
$(0,0,0,0,0,1,0,1,1,1,1,0,1,1,1,0) \xrightarrow{1r} (0,1,0,0,1,1,0,0,1,1,1,0,0,1,1,0)$	10,14	6,8,9,11,13,15	2^{-23}
$(0,0,0,0,0,1,0,1,1,1,1,0,1,1,1,1) \xrightarrow{1r} (1,0,1,1,0,0,1,1,0,0,0,1,1,0,0,0)$	10,14,16,17,18	6,8,9,11,13,15,17,18	$2^{-6.5}$
$(0,0,0,0,0,1,0,1,1,1,1,0,0,0,0) \xrightarrow{1r} (0,1,0,1,1,0,1,1,1,0,0,0,0,1,1,0)$	10,12	6,8,9,11	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,1,1,1,0,0,0,1) \xrightarrow{1r} (1,0,1,0,0,1,0,0,0,1,1,1,1,0,0,0)$	10,12,16,17,18	6,8,9,11,17,18	2^{-12}
$(0,0,0,0,0,1,0,1,1,1,1,0,0,1,0) \xrightarrow{1r} (1,0,0,1,1,0,1,0,1,0,0,0,0,1,1,0)$	10,12,18	6,8,9,11,15,18	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,1,1,1,0,0,1,1) \xrightarrow{1r} (0,1,1,0,0,1,0,1,0,1,1,1,1,0,0,0)$	10,12,16,17	6,8,9,11,15,17	2^{-12}
$(0,0,0,0,0,1,0,1,1,1,1,0,1,0,0) \xrightarrow{1r} (1,0,0,0,0,1,1,0,1,1,1,1,1,0,0,1)$	10,12,14,17,18	6,8,9,11,17,18	2^{-12}
$(0,0,0,0,0,1,0,1,1,1,1,0,1,0,1) \xrightarrow{1r} (0,1,1,1,1,0,0,1,0,0,0,0,0,1,1,1)$	10,12,14,16	6,8,9,11	$2^{-6.5}$
$(0,0,0,0,0,1,0,1,1,1,1,0,1,1,0) \xrightarrow{1r} (0,1,0,0,0,1,1,1,1,1,1,1,1,0,0,1)$	10,12,14,17	6,8,9,11,15,17	2^{-12}
$(0,0,0,0,0,1,0,1,1,1,1,0,1,1,1) \xrightarrow{1r} (1,0,1,1,1,0,0,0,0,0,0,0,0,1,1,1)$	10,12,14,16,18	6,8,9,11,15,18	$2^{-6.5}$
$(0,0,0,0,0,1,0,1,1,1,1,1,0,0,0) \xrightarrow{1r} (1,0,0,0,1,1,1,1,1,1,0,0,0,1,1,0)$	10,12,18	6,8,9,11,13,18	2^{-12}
$(0,0,0,0,0,1,0,1,1,1,1,1,0,0,1) \xrightarrow{1r} (0,1,1,1,0,0,0,0,0,0,0,1,1,1,0,0,0)$	10,12,16,17	6,8,9,11,13,17	$2^{-6.5}$
$(0,0,0,0,0,1,0,1,1,1,1,1,0,1,0) \xrightarrow{1r} (0,1,0,0,1,1,1,0,1,1,0,0,0,1,1,0)$	10,12	6,8,9,11,13,15	2^{-12}
$(0,0,0,0,0,1,0,1,1,1,1,1,0,1,1) \xrightarrow{1r} (1,0,1,1,0,0,0,1,0,0,1,1,1,0,0,0)$	10,12,16,17,18	6,8,9,11,13,15,17,18	$2^{-6.5}$
$(0,0,0,0,0,1,0,1,1,1,1,1,1,0,0) \xrightarrow{1r} (0,1,0,1,0,0,1,0,1,0,1,1,1,0,0,1)$	10,12,14,17	6,8,9,11,13,17	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,1,1,1,1,1,0,1) \xrightarrow{1r} (1,0,1,0,1,1,0,1,0,1,0,1,0,0,0,1,1,1)$	10,12,14,16,18	6,8,9,11,13,18	2^{-12}
$(0,0,0,0,0,1,0,1,1,1,1,1,1,1,0) \xrightarrow{1r} (1,0,0,1,0,0,1,1,1,0,1,1,1,0,0,1)$	10,12,14,17,18	6,8,9,11,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,0,1,1,1,1,1,1,1,1) \xrightarrow{1r} (0,1,1,0,1,1,0,0,0,1,0,0,0,1,1,1)$	10,12,14,16	6,8,9,11,13,15	2^{-12}

Table 0.49 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	7,17	6,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	7,16,18	6,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	7,17,18	6,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	7,16	6,15	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	7,14,18	6,18	2^{-1}
$(0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	7,14,16,17	6,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	7,14	6,15	2^{-1}
$(0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	7,14,16,17,18	6,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	7,17,18	6,13,17,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	7,16	6,13	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	7,17	6,13,15,17	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	7,16,18	6,13,15,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	7,14	6,13	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	7,14,16,17,18	6,13,17,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	7,14,18	6,13,15,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	7,14,16,17	6,13,15,17	2^{-23}
$(0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	7,12,18	6,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	7,12,16,17	6,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	7,12	6,15	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	7,12,16,17,18	6,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	7,12,14,17	6,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	7,12,14,16,18	6,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	7,12,14,17,18	6,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	7,12,14,16	6,15	2^{-23}
$(0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	7,12	6,13	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	7,12,16,17,18	6,13,17,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	7,12,18	6,13,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	7,12,16,17	6,13,15,17	2^{-23}
$(0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	7,12,14,17,18	6,13,17,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	7,12,14,16	6,13	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	7,12,14,17	6,13,15,17	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	7,12,14,16,18	6,13,15,18	$2^{-17.5}$

Table 0.50 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,0,1,1,0,0,0,1,0,0,0,0,0) \xrightarrow{1r} (1,1,0,1,1,0,1,1,0,0,1,0,0,0,1,1)$	7,17,18	6,11,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,0,0,1,0,0,0,0,1) \xrightarrow{1r} (0,0,1,0,0,1,0,0,1,1,0,1,1,1,0,1)$	7,16	6,11	2^{-12}
$(0,0,0,0,0,1,1,0,0,0,1,0,0,0,1,0) \xrightarrow{1r} (0,0,0,1,1,0,1,0,0,0,1,0,0,0,1,1)$	7,17	6,11,15,17	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,0,0,1,0,0,0,1,1) \xrightarrow{1r} (1,1,1,0,0,1,0,1,1,1,0,1,1,1,0,1)$	7,16,18	6,11,15,18	2^{-12}
$(0,0,0,0,0,1,1,0,0,0,1,0,0,1,0,0) \xrightarrow{1r} (0,0,0,0,0,1,1,0,0,1,0,1,1,1,0,0)$	7,14	6,11	2^{-12}
$(0,0,0,0,0,1,1,0,0,0,1,0,0,1,0,1) \xrightarrow{1r} (1,1,1,1,1,0,0,1,1,0,1,0,0,0,1,0)$	7,14,16,17,18	6,11,17,18	$2^{-28.5}$
$(0,0,0,0,0,1,1,0,0,0,1,0,0,1,1,0) \xrightarrow{1r} (1,1,0,0,0,1,1,1,0,1,0,1,1,1,0,0)$	7,14,18	6,11,15,18	2^{-12}
$(0,0,0,0,0,1,1,0,0,0,1,0,0,1,1,1) \xrightarrow{1r} (0,0,1,1,1,0,0,0,1,0,1,0,0,0,1,0)$	7,14,16,17	6,11,15,17	$2^{-28.5}$
$(0,0,0,0,0,1,1,0,0,0,1,0,1,0,0,0) \xrightarrow{1r} (0,0,0,0,1,1,1,1,0,1,1,0,0,0,1,1)$	7,17	6,11,13,17	2^{-23}
$(0,0,0,0,0,1,1,0,0,0,1,0,1,0,0,1) \xrightarrow{1r} (1,1,1,1,0,0,0,0,1,0,0,1,1,1,0,1)$	7,16,18	6,11,13,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,0,0,1,0,1,0,1,0) \xrightarrow{1r} (1,1,0,0,1,1,1,0,0,1,1,0,0,0,1,1)$	7,17,18	6,11,13,15,17,18	2^{-23}
$(0,0,0,0,0,1,1,0,0,0,1,0,1,0,1,1) \xrightarrow{1r} (0,0,1,1,0,0,0,1,1,0,0,1,1,1,0,1)$	7,16	6,11,13,15	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,0,0,1,0,1,1,0,0) \xrightarrow{1r} (1,1,0,1,0,0,1,0,0,0,0,1,1,1,0,0)$	7,14,18	6,11,13,18	$2^{-6.5}$
$(0,0,0,0,0,1,1,0,0,0,1,0,1,1,0,1) \xrightarrow{1r} (0,0,1,0,1,1,0,1,1,1,1,0,0,0,1,0)$	7,14,16,17	6,11,13,17	2^{-23}
$(0,0,0,0,0,1,1,0,0,0,1,0,1,1,1,0) \xrightarrow{1r} (0,0,0,1,0,0,1,1,0,0,0,1,1,1,0,0)$	7,14	6,11,13,15	$2^{-6.5}$
$(0,0,0,0,0,1,1,0,0,0,1,0,1,1,1,1) \xrightarrow{1r} (1,1,1,0,1,1,0,0,1,1,1,0,0,0,1,0)$	7,14,16,17,18	6,11,13,15,17,18	2^{-23}
$(0,0,0,0,0,1,1,0,0,0,1,1,0,0,0,0) \xrightarrow{1r} (0,0,0,0,0,1,0,0,0,1,1,1,1,1,0,0)$	7,12	6,11	2^{-12}
$(0,0,0,0,0,1,1,0,0,0,1,1,0,0,0,1) \xrightarrow{1r} (1,1,1,1,1,0,1,1,1,0,0,0,0,0,1,0)$	7,12,16,17,18	6,11,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,0,0,1,1,0,0,1,0) \xrightarrow{1r} (1,1,0,0,0,1,0,1,0,1,1,1,1,1,0,0)$	7,12,18	6,11,15,18	2^{-12}
$(0,0,0,0,0,1,1,0,0,0,1,1,0,0,1,1) \xrightarrow{1r} (0,0,1,1,1,0,1,0,1,0,0,0,0,0,1,0)$	7,12,16,17	6,11,15,17	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,0,0,1,1,0,1,0,0) \xrightarrow{1r} (1,1,0,1,1,0,0,1,0,0,0,0,0,0,1,1)$	7,12,14,17,18	6,11,17,18	$2^{-6.5}$
$(0,0,0,0,0,1,1,0,0,0,1,1,0,1,0,1) \xrightarrow{1r} (0,0,1,0,0,1,1,0,1,1,1,1,1,1,0,1)$	7,12,14,16	6,11	2^{-12}
$(0,0,0,0,0,1,1,0,0,0,1,1,0,1,1,0) \xrightarrow{1r} (0,0,0,1,1,0,0,0,0,0,0,0,0,0,1,1)$	7,12,14,17	6,11,15,17	$2^{-6.5}$
$(0,0,0,0,0,1,1,0,0,0,1,1,0,1,1,1) \xrightarrow{1r} (1,1,1,0,0,1,1,1,1,1,1,1,1,1,0,1)$	7,12,14,16,18	6,11,15,18	2^{-12}
$(0,0,0,0,0,1,1,0,0,0,1,1,1,0,0,0) \xrightarrow{1r} (1,1,0,1,0,0,0,0,0,0,0,1,1,1,1,0,0)$	7,12,18	6,11,13,18	$2^{-6.5}$
$(0,0,0,0,0,1,1,0,0,0,1,1,1,0,0,1) \xrightarrow{1r} (0,0,1,0,1,1,1,1,1,1,1,0,0,0,1,0)$	7,12,16,17	6,11,13,17	2^{-12}
$(0,0,0,0,0,1,1,0,0,0,1,1,1,0,1,0) \xrightarrow{1r} (0,0,0,1,0,0,0,1,0,0,1,1,1,1,0,0)$	7,12	6,11,13,15	$2^{-6.5}$
$(0,0,0,0,0,1,1,0,0,0,1,1,1,0,1,1) \xrightarrow{1r} (1,1,1,0,1,1,1,0,1,1,0,0,0,0,1,0)$	7,12,16,17,18	6,11,13,15,17,18	2^{-12}
$(0,0,0,0,0,1,1,0,0,0,1,1,1,1,0,0) \xrightarrow{1r} (0,0,0,0,1,1,0,1,0,1,0,1,0,0,0,1,1)$	7,12,14,17	6,11,13,17	2^{-12}
$(0,0,0,0,0,1,1,0,0,0,1,1,1,1,0,1) \xrightarrow{1r} (1,1,1,1,0,0,1,0,1,0,1,1,1,1,0,1)$	7,12,14,16,18	6,11,13,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,0,0,1,1,1,1,1,0) \xrightarrow{1r} (1,1,0,0,1,1,0,0,0,1,0,0,0,0,1,1)$	7,12,14,17,18	6,11,13,15,17,18	2^{-12}
$(0,0,0,0,0,1,1,0,0,0,1,1,1,1,1,1) \xrightarrow{1r} (0,0,1,1,0,0,1,1,1,0,1,1,1,1,0,1)$	7,12,14,16	6,11,13,15	$2^{-17.5}$

Table 0.51 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,0,1,1,0,0,1,0,0,0,0,0,0) \xrightarrow{1r} (1,1,1,0,1,0,1,0,0,0,1,0,0,1,0,0)$	7,10,18	6,18	2^{-23}
$(0,0,0,0,0,1,1,0,0,1,0,0,0,0,0,1) \xrightarrow{1r} (0,0,0,1,0,1,0,1,1,1,0,1,1,0,1,0)$	7,10,16,17	6,17	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,0,1,0,0,0,0,1,0) \xrightarrow{1r} (0,0,1,0,1,0,1,1,0,0,1,0,0,1,0,0)$	7,10	6,15	2^{-23}
$(0,0,0,0,0,1,1,0,0,1,0,0,0,0,1,1) \xrightarrow{1r} (1,1,0,1,0,1,0,0,1,1,0,1,1,0,1,0)$	7,10,16,17,18	6,15,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,0,1,0,0,0,1,0,0) \xrightarrow{1r} (0,0,1,1,0,1,1,1,0,1,0,1,1,0,1,1)$	7,10,14,17	6,17	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,0,1,0,0,0,1,0,1) \xrightarrow{1r} (1,1,0,0,1,0,0,0,1,0,1,0,0,1,0,1)$	7,10,14,16,18	6,18	2^{-34}
$(0,0,0,0,0,1,1,0,0,1,0,0,0,1,1,0) \xrightarrow{1r} (1,1,1,1,0,1,1,0,0,1,0,1,1,0,1,1)$	7,10,14,17,18	6,15,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,0,1,0,0,0,1,1,1) \xrightarrow{1r} (0,0,0,0,1,0,0,1,1,0,1,0,0,1,0,1)$	7,10,14,16	6,15	2^{-34}
$(0,0,0,0,0,1,1,0,0,1,0,0,1,0,0,0) \xrightarrow{1r} (0,0,1,1,1,1,0,0,1,1,0,0,1,0,0,0)$	7,10	6,13	$2^{-28.5}$
$(0,0,0,0,0,1,1,0,0,1,0,0,1,0,0,1) \xrightarrow{1r} (1,1,0,0,0,0,0,1,1,0,0,1,1,0,1,0)$	7,10,16,17,18	6,13,17,18	2^{-23}
$(0,0,0,0,0,1,1,0,0,1,0,0,1,0,1,0) \xrightarrow{1r} (1,1,1,1,1,1,1,0,1,1,0,1,1,0,0,0)$	7,10,18	6,13,15,18	$2^{-28.5}$
$(0,0,0,0,0,1,1,0,0,1,0,0,1,0,1,1) \xrightarrow{1r} (0,0,0,0,0,0,0,0,1,0,0,1,1,0,1,0)$	7,10,16,17	6,13,15,17	2^{-23}
$(0,0,0,0,0,1,1,0,0,1,0,0,1,1,0,0) \xrightarrow{1r} (1,1,1,0,0,0,1,1,0,0,0,1,1,0,1,1)$	7,10,14,17,18	6,13,17,18	2^{-12}
$(0,0,0,0,0,1,1,0,0,1,0,0,1,1,0,1) \xrightarrow{1r} (0,0,0,1,1,1,0,0,1,1,1,0,0,1,0,1)$	7,10,14,16	6,13	$2^{-28.5}$
$(0,0,0,0,0,1,1,0,0,1,0,0,1,1,1,0) \xrightarrow{1r} (0,0,1,0,0,0,1,0,0,0,0,1,1,0,1,1)$	7,10,14,17	6,13,15,17	2^{-12}
$(0,0,0,0,0,1,1,0,0,1,0,0,1,1,1,1) \xrightarrow{1r} (1,1,0,1,1,1,0,1,1,1,1,0,0,1,0,1)$	7,10,14,16,18	6,13,15,18	$2^{-28.5}$
$(0,0,0,0,0,1,1,0,0,1,0,1,0,0,0,0) \xrightarrow{1r} (0,0,1,1,0,1,0,1,0,1,1,1,1,0,1,1)$	7,10,12,17	6,17	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,0,1,0,1,0,0,0,1) \xrightarrow{1r} (1,1,0,0,1,0,1,0,1,0,0,0,0,1,0,1)$	7,10,12,16,18	6,18	2^{-23}
$(0,0,0,0,0,1,1,0,0,1,0,1,0,0,1,0) \xrightarrow{1r} (1,1,1,1,0,1,0,0,0,1,1,1,1,0,1,1)$	7,10,12,17,18	6,15,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,0,1,0,1,0,0,1,1) \xrightarrow{1r} (0,0,0,0,1,0,1,1,1,0,0,0,0,1,0,1)$	7,10,12,16	6,15	2^{-23}
$(0,0,0,0,0,1,1,0,0,1,0,1,0,1,0,0) \xrightarrow{1r} (1,1,1,0,1,0,0,0,0,0,0,0,0,1,0,0)$	7,10,12,14,18	6,18	2^{-12}
$(0,0,0,0,0,1,1,0,0,1,0,1,0,1,0,1) \xrightarrow{1r} (0,0,0,1,0,1,1,1,1,1,1,1,1,0,1,0)$	7,10,12,14,16,17	6,17	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,0,1,0,1,0,1,1,0) \xrightarrow{1r} (0,0,1,0,1,0,0,1,0,0,0,0,0,1,0,0)$	7,10,12,14	6,15	2^{-12}
$(0,0,0,0,0,1,1,0,0,1,0,1,0,1,1,1) \xrightarrow{1r} (1,1,0,1,0,1,1,0,1,1,1,1,1,0,1,0)$	7,10,12,14,16,17,18	6,15,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,0,1,0,1,1,0,0,0) \xrightarrow{1r} (1,1,1,0,0,0,0,1,0,0,1,1,1,0,1,1)$	7,10,12,17,18	6,13,17,18	2^{-12}
$(0,0,0,0,0,1,1,0,0,1,0,1,1,0,0,1) \xrightarrow{1r} (0,0,0,1,1,1,1,0,1,1,1,0,0,0,1,0,1)$	7,10,12,16	6,13	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,0,1,0,1,1,0,1,0) \xrightarrow{1r} (0,0,1,0,0,0,0,0,0,0,0,1,1,1,0,1,1)$	7,10,12,17	6,13,15,17	2^{-12}
$(0,0,0,0,0,1,1,0,0,1,0,1,1,0,1,1) \xrightarrow{1r} (1,1,0,1,1,1,1,1,1,1,1,0,0,0,1,0,1)$	7,10,12,16,18	6,13,15,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,0,1,0,1,1,1,0,0) \xrightarrow{1r} (0,0,1,1,1,1,0,0,0,1,0,0,0,1,0,0)$	7,10,12,14	6,13	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,0,1,0,1,1,1,0,1) \xrightarrow{1r} (1,1,0,0,0,0,1,1,1,0,1,1,1,0,1,0)$	7,10,12,14,16,17,18	6,13,17,18	2^{-23}
$(0,0,0,0,0,1,1,0,0,1,0,1,1,1,1,0) \xrightarrow{1r} (1,1,1,1,1,1,0,1,0,1,0,0,0,1,0,0)$	7,10,12,14,18	6,13,15,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,0,1,0,1,1,1,1,1) \xrightarrow{1r} (0,0,0,0,0,0,1,0,1,0,1,1,1,0,1,0)$	7,10,12,14,16,17	6,13,15,17	2^{-23}

Table 0.52 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,0,1,1,0,0,1,1,0,0,0,0,0) \xrightarrow{1r} (0,0,1,0,1,1,1,0,0,1,1,1,0,1,0,0)$	7,10	6,11	2^{-23}
$(0,0,0,0,0,1,1,0,0,1,1,0,0,0,0,1) \xrightarrow{1r} (1,1,0,1,0,0,0,1,1,0,0,0,1,0,1,0)$	7,10,16,17,18	6,11,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,0,1,1,0,0,0,1,0) \xrightarrow{1r} (1,1,1,0,1,1,1,1,0,1,1,1,0,1,0,0)$	7,10,18	6,11,15,18	2^{-23}
$(0,0,0,0,0,1,1,0,0,1,1,0,0,0,1,1) \xrightarrow{1r} (0,0,0,1,0,0,0,0,1,0,0,0,1,0,1,0)$	7,10,16,17	6,11,15,17	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,0,1,1,0,0,1,0,0) \xrightarrow{1r} (1,1,1,1,0,0,1,1,0,0,0,0,1,0,1,1)$	7,10,14,17,18	6,11,17,18	$2^{-6.5}$
$(0,0,0,0,0,1,1,0,0,1,1,0,0,1,0,1) \xrightarrow{1r} (0,0,0,0,1,1,0,0,1,1,1,1,0,1,0,1)$	7,10,14,16	6,11	2^{-23}
$(0,0,0,0,0,1,1,0,0,1,1,0,0,1,1,0) \xrightarrow{1r} (0,0,1,1,0,0,1,0,0,0,0,0,1,0,1,1)$	7,10,14,17	6,11,15,17	$2^{-6.5}$
$(0,0,0,0,0,1,1,0,0,1,1,0,0,1,1,1) \xrightarrow{1r} (1,1,0,0,1,1,0,1,1,1,1,1,0,1,0,1)$	7,10,14,16,18	6,11,15,18	2^{-23}
$(0,0,0,0,0,1,1,0,0,1,1,0,1,0,0,0) \xrightarrow{1r} (1,1,1,1,1,0,1,0,0,0,1,1,0,1,0,0)$	7,10,18	6,11,13,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,0,1,1,0,1,0,0,1) \xrightarrow{1r} (0,0,0,0,0,1,0,1,1,1,0,0,1,0,1,0)$	7,10,16,17	6,11,13,17	2^{-12}
$(0,0,0,0,0,1,1,0,0,1,1,0,1,0,1,0) \xrightarrow{1r} (0,0,1,1,1,0,1,1,0,0,1,1,0,1,0,0)$	7,10	6,11,13,15	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,0,1,1,0,1,0,1,1) \xrightarrow{1r} (1,1,0,0,0,1,0,0,1,1,1,0,0,1,0,1,0)$	7,10,16,17,18	6,11,13,15,17,18	2^{-12}
$(0,0,0,0,0,1,1,0,0,1,1,0,1,1,0,0) \xrightarrow{1r} (0,0,1,0,0,1,1,1,0,1,0,0,1,0,1,1)$	7,10,14,17	6,11,13,17	2^{-12}
$(0,0,0,0,0,1,1,0,0,1,1,0,1,1,0,1) \xrightarrow{1r} (1,1,0,1,1,0,0,0,1,0,1,1,0,1,0,1)$	7,10,14,16,18	6,11,13,18	$2^{-28.5}$
$(0,0,0,0,0,1,1,0,0,1,1,0,1,1,1,0) \xrightarrow{1r} (1,1,1,0,0,1,1,0,0,1,0,0,1,0,1,1)$	7,10,14,17,18	6,11,13,15,17,18	2^{-12}
$(0,0,0,0,0,1,1,0,0,1,1,0,1,1,1,1) \xrightarrow{1r} (0,0,0,1,1,0,0,1,1,0,1,1,0,1,0,1)$	7,10,14,16	6,11,13,15	$2^{-28.5}$
$(0,0,0,0,0,1,1,0,0,1,1,1,0,0,0,0) \xrightarrow{1r} (1,1,1,1,0,0,0,1,0,0,1,0,1,0,1,1)$	7,10,12,17,18	6,11,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,0,1,1,1,0,0,0,1) \xrightarrow{1r} (0,0,0,0,1,1,1,0,1,1,0,1,0,1,0,1)$	7,10,12,16	6,11	2^{-23}
$(0,0,0,0,0,1,1,0,0,1,1,1,0,0,1,0) \xrightarrow{1r} (0,0,1,1,0,0,0,0,0,0,1,0,1,0,1,1)$	7,10,12,17	6,11,15,17	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,0,1,1,1,0,0,1,1) \xrightarrow{1r} (1,1,0,0,1,1,1,1,1,1,0,1,0,1,0,1)$	7,10,12,16,18	6,11,15,18	2^{-23}
$(0,0,0,0,0,1,1,0,0,1,1,1,0,1,0,0) \xrightarrow{1r} (0,0,1,0,1,1,0,0,0,1,0,1,0,1,0,0)$	7,10,12,14	6,11	2^{-23}
$(0,0,0,0,0,1,1,0,0,1,1,1,0,1,0,1) \xrightarrow{1r} (1,1,0,1,0,0,1,1,1,0,1,0,1,0,1,0)$	7,10,12,14,16,17,18	6,11,17,18	$2^{-28.5}$
$(0,0,0,0,0,1,1,0,0,1,1,1,0,1,1,0) \xrightarrow{1r} (1,1,1,0,1,1,0,1,0,1,0,1,0,1,0,0)$	7,10,12,14,18	6,11,15,18	2^{-23}
$(0,0,0,0,0,1,1,0,0,1,1,1,0,1,1,1) \xrightarrow{1r} (0,0,0,1,0,0,1,0,1,0,1,0,1,0,1,0)$	7,10,12,14,16,17	6,11,15,17	$2^{-28.5}$
$(0,0,0,0,0,1,1,0,0,1,1,1,1,0,0,0) \xrightarrow{1r} (0,0,1,0,0,1,0,1,0,1,1,0,1,0,1,1)$	7,10,12,17	6,11,13,17	2^{-23}
$(0,0,0,0,0,1,1,0,0,1,1,1,1,0,0,1) \xrightarrow{1r} (1,1,0,1,1,0,1,0,1,0,1,0,0,1,0,1)$	7,10,12,16,18	6,11,13,18	$2^{-28.5}$
$(0,0,0,0,0,1,1,0,0,1,1,1,1,0,1,0) \xrightarrow{1r} (1,1,1,1,1,0,0,0,0,0,0,1,0,1,0,0)$	7,10,12,14,18	6,11,13,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,0,1,1,1,1,1,0,1) \xrightarrow{1r} (0,0,0,0,0,1,1,1,1,1,1,0,1,0,1,0)$	7,10,12,14,16,17	6,11,13,17	2^{-23}
$(0,0,0,0,0,1,1,0,0,1,1,1,1,1,1,0) \xrightarrow{1r} (0,0,1,1,1,0,0,1,0,0,0,1,0,1,0,0)$	7,10,12,14	6,11,13,15	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,0,1,1,1,1,1,1,1) \xrightarrow{1r} (1,1,0,0,0,1,1,0,1,1,1,0,1,0,1,0)$	7,10,12,14,16,17,18	6,11,13,15,17,18	2^{-23}

Table 0.53 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,0,1,1,0,1,0,0,0,0,0,0,0) \xrightarrow{1r} (1,0,0,0,1,0,1,0,0,0,1,0,0,1,1,1)$	7,17,18	6,9,17,18	2^{-23}
$(0,0,0,0,0,1,1,0,1,0,0,0,0,0,0,1) \xrightarrow{1r} (0,1,1,1,0,1,0,1,1,1,0,1,1,0,0,1)$	7,16	6,9	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,1,0,0,0,0,0,1,0) \xrightarrow{1r} (0,1,0,0,1,0,1,1,0,0,1,0,0,1,1,1)$	7,17	6,9,15,17	2^{-23}
$(0,0,0,0,0,1,1,0,1,0,0,0,0,0,1,1) \xrightarrow{1r} (1,0,1,1,0,1,0,0,1,1,0,1,1,0,0,1)$	7,16,18	6,9,15,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,1,0,0,0,0,1,0,0) \xrightarrow{1r} (0,1,0,1,0,1,1,1,0,1,0,1,1,0,0,0)$	7,14	6,9	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,1,0,0,0,0,1,0,1) \xrightarrow{1r} (1,0,1,0,1,0,0,0,1,0,1,0,0,1,1,0)$	7,14,16,17,18	6,9,17,18	2^{-34}
$(0,0,0,0,0,1,1,0,1,0,0,0,0,1,1,0) \xrightarrow{1r} (1,0,0,1,0,1,1,0,0,1,0,1,1,0,0,0)$	7,14,18	6,9,15,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,1,0,0,0,0,1,1,1) \xrightarrow{1r} (0,1,1,0,1,0,0,1,1,0,1,0,0,1,1,0)$	7,14,16,17	6,9,15,17	2^{-34}
$(0,0,0,0,0,1,1,0,1,0,0,0,1,0,0,0) \xrightarrow{1r} (0,1,0,1,1,1,1,0,0,1,1,0,0,1,1,1)$	7,17	6,9,13,17	$2^{-28.5}$
$(0,0,0,0,0,1,1,0,1,0,0,0,1,0,0,1) \xrightarrow{1r} (1,0,1,0,0,0,0,1,1,0,0,1,1,0,0,1)$	7,16,18	6,9,13,18	2^{-23}
$(0,0,0,0,0,1,1,0,1,0,0,0,1,0,1,0) \xrightarrow{1r} (1,0,0,1,1,1,1,1,0,1,1,0,0,1,1,1)$	7,17,18	6,9,13,15,17,18	$2^{-28.5}$
$(0,0,0,0,0,1,1,0,1,0,0,0,1,0,1,1) \xrightarrow{1r} (0,1,1,0,0,0,0,1,0,0,1,1,0,0,1)$	7,16	6,9,13,15	2^{-23}
$(0,0,0,0,0,1,1,0,1,0,0,0,1,1,0,0) \xrightarrow{1r} (1,0,0,0,0,0,1,1,0,0,0,1,1,0,0,0)$	7,14,18	6,9,13,18	2^{-12}
$(0,0,0,0,0,1,1,0,1,0,0,0,1,1,0,1) \xrightarrow{1r} (0,1,1,1,1,1,0,0,1,1,1,0,0,1,1,0)$	7,14,16,17	6,9,13,17	$2^{-28.5}$
$(0,0,0,0,0,1,1,0,1,0,0,0,1,1,1,0) \xrightarrow{1r} (0,1,0,0,0,0,1,0,0,0,0,1,1,0,0,0)$	7,14	6,9,13,15	2^{-12}
$(0,0,0,0,0,1,1,0,1,0,0,0,1,1,1,1) \xrightarrow{1r} (1,0,1,1,1,1,0,1,1,1,1,0,0,1,1,0)$	7,14,16,17,18	6,9,13,15,17,18	$2^{-28.5}$
$(0,0,0,0,0,1,1,0,1,0,0,1,0,0,0,0) \xrightarrow{1r} (0,1,0,1,0,1,0,1,0,1,1,1,1,0,0,0)$	7,12	6,9	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,1,0,0,1,0,0,0,1) \xrightarrow{1r} (1,0,1,0,1,0,1,0,1,0,0,0,0,1,1,0)$	7,12,16,17,18	6,9,17,18	2^{-23}
$(0,0,0,0,0,1,1,0,1,0,0,1,0,0,1,0) \xrightarrow{1r} (1,0,0,1,0,1,0,0,0,1,1,1,1,0,0,0)$	7,12,18	6,9,15,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,1,0,0,1,0,0,1,1) \xrightarrow{1r} (0,1,1,0,1,0,1,1,1,0,0,0,0,1,1,0)$	7,12,16,17	6,9,15,17	2^{-23}
$(0,0,0,0,0,1,1,0,1,0,0,1,0,1,0,0) \xrightarrow{1r} (1,0,0,0,1,0,0,0,0,0,0,0,0,1,1,1)$	7,12,14,17,18	6,9,17,18	2^{-12}
$(0,0,0,0,0,1,1,0,1,0,0,1,0,1,0,1) \xrightarrow{1r} (0,1,1,1,0,1,1,1,1,1,1,1,1,0,0,1)$	7,12,14,16	6,9	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,1,0,0,1,0,1,1,0) \xrightarrow{1r} (0,1,0,0,1,0,0,1,0,0,0,0,0,1,1,1)$	7,12,14,17	6,9,15,17	2^{-12}
$(0,0,0,0,0,1,1,0,1,0,0,1,0,1,1,1) \xrightarrow{1r} (1,0,1,1,0,1,1,0,1,1,1,1,1,0,0,1)$	7,12,14,16,18	6,9,15,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,1,0,0,1,1,0,0,0) \xrightarrow{1r} (1,0,0,0,0,0,0,1,0,0,1,1,1,0,0,0)$	7,12,18	6,9,13,18	2^{-12}
$(0,0,0,0,0,1,1,0,1,0,0,1,1,0,0,1) \xrightarrow{1r} (0,1,1,1,1,1,1,0,1,1,0,0,0,1,1,0)$	7,12,16,17	6,9,13,17	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,1,0,0,1,1,0,1,0) \xrightarrow{1r} (0,1,0,0,0,0,0,0,0,0,0,1,1,1,0,0,0)$	7,12	6,9,13,15	2^{-12}
$(0,0,0,0,0,1,1,0,1,0,0,1,1,0,1,1) \xrightarrow{1r} (1,0,1,1,1,1,1,1,1,1,0,0,0,1,1,0)$	7,12,16,17,18	6,9,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,1,0,0,1,1,1,0,0) \xrightarrow{1r} (0,1,0,1,1,1,0,0,0,1,0,0,0,1,1,1)$	7,12,14,17	6,9,13,17	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,1,0,0,1,1,1,0,1) \xrightarrow{1r} (1,0,1,0,0,0,1,1,1,0,1,1,1,0,0,1)$	7,12,14,16,18	6,9,13,18	2^{-23}
$(0,0,0,0,0,1,1,0,1,0,0,1,1,1,1,0) \xrightarrow{1r} (1,0,0,1,1,1,0,1,0,1,0,0,0,1,1,1)$	7,12,14,17,18	6,9,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,1,0,0,1,1,1,1,1) \xrightarrow{1r} (0,1,1,0,0,0,1,0,1,0,1,1,1,0,0,1)$	7,12,14,16	6,9,13,15	2^{-23}

Table 0.54 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,0,1,1,0,1,0,1,0,0,0,0,0) \xrightarrow{1r} (0,1,0,0,1,1,1,0,0,1,1,1,0,1,1,1)$	7,17	6,9,11,17	2^{-23}
$(0,0,0,0,0,1,1,0,1,0,1,0,0,0,0,1) \xrightarrow{1r} (1,0,1,1,0,0,0,1,1,0,0,0,1,0,0,1)$	7,16,18	6,9,11,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,1,0,1,0,0,0,1,0) \xrightarrow{1r} (1,0,0,0,1,1,1,1,0,1,1,1,0,1,1,1)$	7,17,18	6,9,11,15,17,18	2^{-23}
$(0,0,0,0,0,1,1,0,1,0,1,0,0,0,1,1) \xrightarrow{1r} (0,1,1,1,0,0,0,0,1,0,0,0,1,0,0,1)$	7,16	6,9,11,15	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,1,0,1,0,0,1,0,0) \xrightarrow{1r} (1,0,0,1,0,0,1,1,0,0,0,0,1,0,0,0)$	7,14,18	6,9,11,18	$2^{-6.5}$
$(0,0,0,0,0,1,1,0,1,0,1,0,0,1,0,1) \xrightarrow{1r} (0,1,1,0,1,1,0,0,1,1,1,1,0,1,1,0)$	7,14,16,17	6,9,11,17	2^{-23}
$(0,0,0,0,0,1,1,0,1,0,1,0,0,1,1,0) \xrightarrow{1r} (0,1,0,1,0,0,1,0,0,0,0,0,0,1,0,0,0)$	7,14	6,9,11,15	$2^{-6.5}$
$(0,0,0,0,0,1,1,0,1,0,1,0,0,1,1,1) \xrightarrow{1r} (1,0,1,0,1,1,0,0,1,1,1,1,1,0,1,1,0)$	7,14,16,17,18	6,9,11,15,17,18	2^{-23}
$(0,0,0,0,0,1,1,0,1,0,1,0,1,0,0,0) \xrightarrow{1r} (1,0,0,1,1,0,1,0,0,0,1,1,0,1,1,1)$	7,17,18	6,9,11,13,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,1,0,1,0,1,0,0,1) \xrightarrow{1r} (0,1,1,0,0,1,0,1,1,1,0,0,1,0,0,1)$	7,16	6,9,11,13	2^{-12}
$(0,0,0,0,0,1,1,0,1,0,1,0,1,0,1,0) \xrightarrow{1r} (0,1,0,1,1,0,1,1,0,0,1,1,0,1,1,1)$	7,17	6,9,11,13,15,17	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,1,0,1,0,1,0,1,1) \xrightarrow{1r} (1,0,1,0,0,1,0,0,1,1,0,0,1,0,0,1)$	7,16,18	6,9,11,13,15,18	2^{-12}
$(0,0,0,0,0,1,1,0,1,0,1,0,1,1,0,0) \xrightarrow{1r} (0,1,0,0,0,1,1,1,0,1,0,0,1,0,0,0)$	7,14	6,9,11,13	2^{-12}
$(0,0,0,0,0,1,1,0,1,0,1,0,1,1,0,1) \xrightarrow{1r} (1,0,1,1,1,0,0,0,1,0,1,1,0,1,1,0)$	7,14,16,17,18	6,9,11,13,17,18	$2^{-28.5}$
$(0,0,0,0,0,1,1,0,1,0,1,0,1,1,1,0) \xrightarrow{1r} (1,0,0,0,0,1,1,0,0,1,0,0,1,0,0,0)$	7,14,18	6,9,11,13,15,18	2^{-12}
$(0,0,0,0,0,1,1,0,1,0,1,0,1,1,1,1) \xrightarrow{1r} (0,1,1,1,1,0,0,1,1,0,1,1,0,1,1,0)$	7,14,16,17	6,9,11,13,15,17	$2^{-28.5}$
$(0,0,0,0,0,1,1,0,1,0,1,0,1,0,0,0) \xrightarrow{1r} (1,0,0,1,0,0,0,1,0,0,1,0,1,0,0,0)$	7,12,18	6,9,11,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,1,0,1,0,1,0,0,1) \xrightarrow{1r} (0,1,1,0,1,1,1,0,1,1,0,1,0,1,1,0)$	7,12,16,17	6,9,11,17	2^{-23}
$(0,0,0,0,0,1,1,0,1,0,1,0,1,0,1,0) \xrightarrow{1r} (0,1,0,1,0,0,0,0,0,0,0,1,0,1,0,0,0)$	7,12	6,9,11,15	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,1,0,1,0,1,0,0,1) \xrightarrow{1r} (1,0,1,0,1,1,1,1,1,1,0,1,0,1,1,0)$	7,12,16,17,18	6,9,11,15,17,18	2^{-23}
$(0,0,0,0,0,1,1,0,1,0,1,0,1,0,1,0) \xrightarrow{1r} (0,1,0,0,1,1,0,0,0,1,0,1,0,1,1,1)$	7,12,14,17	6,9,11,17	2^{-23}
$(0,0,0,0,0,1,1,0,1,0,1,0,1,0,1,0) \xrightarrow{1r} (1,0,1,1,0,0,1,1,1,0,1,0,1,0,0,1)$	7,12,14,16,18	6,9,11,18	$2^{-28.5}$
$(0,0,0,0,0,1,1,0,1,0,1,0,1,0,1,1) \xrightarrow{1r} (1,0,0,0,1,1,0,1,0,1,0,1,0,1,1,1)$	7,12,14,17,18	6,9,11,15,17,18	2^{-23}
$(0,0,0,0,0,1,1,0,1,0,1,0,1,0,1,1) \xrightarrow{1r} (0,1,1,1,0,0,1,0,1,0,1,0,1,0,0,1)$	7,12,14,16	6,9,11,15	$2^{-28.5}$
$(0,0,0,0,0,1,1,0,1,0,1,0,1,1,0,0,0) \xrightarrow{1r} (0,1,0,0,0,1,0,1,0,1,1,0,1,0,0,0)$	7,12	6,9,11,13	2^{-23}
$(0,0,0,0,0,1,1,0,1,0,1,0,1,1,0,0,1) \xrightarrow{1r} (1,0,1,1,1,0,1,0,1,0,1,0,0,1,0,1,0)$	7,12,16,17,18	6,9,11,13,17,18	$2^{-28.5}$
$(0,0,0,0,0,1,1,0,1,0,1,0,1,1,0,1,0) \xrightarrow{1r} (1,0,0,0,0,1,0,0,0,1,1,0,1,0,0,0,0)$	7,12,18	6,9,11,13,15,18	2^{-23}
$(0,0,0,0,0,1,1,0,1,0,1,0,1,1,0,1,1) \xrightarrow{1r} (0,1,1,1,1,0,1,1,1,0,0,1,0,1,1,0,0)$	7,12,16,17	6,9,11,13,15,17	$2^{-28.5}$
$(0,0,0,0,0,1,1,0,1,0,1,0,1,1,1,0,0) \xrightarrow{1r} (1,0,0,1,1,0,0,0,0,0,0,0,1,0,1,1,1)$	7,12,14,17,18	6,9,11,13,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,1,0,1,0,1,1,1,0,1) \xrightarrow{1r} (0,1,1,0,0,1,1,1,1,1,1,1,0,1,0,0,1)$	7,12,14,16	6,9,11,13	2^{-23}
$(0,0,0,0,0,1,1,0,1,0,1,0,1,1,1,1,0) \xrightarrow{1r} (0,1,0,1,1,0,0,1,0,0,0,1,0,0,1,1,1)$	7,12,14,17	6,9,11,13,15,17	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,1,0,1,0,1,1,1,1,1) \xrightarrow{1r} (1,0,1,0,0,1,1,0,1,1,1,0,1,0,0,0,1)$	7,12,14,16,18	6,9,11,13,15,18	2^{-23}

Table 0.55 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,0,1,1,0,1,1,0,0,0,0,0,0) \xrightarrow{1r} (0,1,1,1,1,1,1,0,1,1,1,0,0,0,0,0)$	7,10	6,9	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,1,1,0,0,0,0,0,1) \xrightarrow{1r} (1,0,0,0,0,0,0,0,1,0,0,0,1,1,1,0)$	7,10,16,17,18	6,9,17,18	2^{-12}
$(0,0,0,0,0,1,1,0,1,1,0,0,0,0,1,0) \xrightarrow{1r} (1,0,1,1,1,1,1,0,0,1,1,1,0,0,0,0)$	7,10,18	6,9,15,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,1,1,0,0,0,0,1,1) \xrightarrow{1r} (0,1,0,0,0,0,0,1,1,0,0,0,1,1,1,0)$	7,10,16,17	6,9,15,17	2^{-12}
$(0,0,0,0,0,1,1,0,1,1,0,0,0,1,0,0) \xrightarrow{1r} (1,0,1,0,0,0,1,0,0,0,0,0,1,1,1,1)$	7,10,14,17,18	6,9,17,18	2^{-1}
$(0,0,0,0,0,1,1,0,1,1,0,0,0,1,0,1) \xrightarrow{1r} (0,1,0,1,1,1,0,1,1,1,1,1,0,0,0,1)$	7,10,14,16	6,9	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,1,1,0,0,0,1,1,0) \xrightarrow{1r} (0,1,1,0,0,0,1,1,0,0,0,0,1,1,1,1)$	7,10,14,17	6,9,15,17	2^{-1}
$(0,0,0,0,0,1,1,0,1,1,0,0,0,1,1,1) \xrightarrow{1r} (1,0,0,1,1,1,0,0,1,1,1,1,0,0,0,1)$	7,10,14,16,18	6,9,15,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,1,1,0,0,1,0,0,0) \xrightarrow{1r} (1,0,1,0,1,0,1,1,0,0,1,1,0,0,0,0)$	7,10,18	6,9,13,18	2^{-12}
$(0,0,0,0,0,1,1,0,1,1,0,0,1,0,0,1) \xrightarrow{1r} (0,1,0,1,0,1,0,0,1,1,0,0,1,1,1,0)$	7,10,16,17	6,9,13,17	$2^{-6.5}$
$(0,0,0,0,0,1,1,0,1,1,0,0,1,0,1,0) \xrightarrow{1r} (0,1,1,0,1,0,1,0,0,0,1,1,0,0,0,0)$	7,10	6,9,13,15	2^{-12}
$(0,0,0,0,0,1,1,0,1,1,0,0,1,0,1,1) \xrightarrow{1r} (1,0,0,1,0,1,0,1,1,1,1,0,0,1,1,0)$	7,10,16,17,18	6,9,13,15,17,18	$2^{-6.5}$
$(0,0,0,0,0,1,1,0,1,1,0,0,1,1,0,0) \xrightarrow{1r} (0,1,1,1,0,1,1,0,0,1,0,0,1,1,1,1)$	7,10,14,17	6,9,13,17	$2^{-6.5}$
$(0,0,0,0,0,1,1,0,1,1,0,0,1,1,0,1) \xrightarrow{1r} (1,0,0,0,1,0,0,1,1,0,1,1,0,0,0,1)$	7,10,14,16,18	6,9,13,18	2^{-23}
$(0,0,0,0,0,1,1,0,1,1,0,0,1,1,1,0) \xrightarrow{1r} (1,0,1,1,0,1,1,1,0,1,0,0,1,1,1,1)$	7,10,14,17,18	6,9,13,15,17,18	$2^{-6.5}$
$(0,0,0,0,0,1,1,0,1,1,0,0,1,1,1,1) \xrightarrow{1r} (0,1,0,0,1,0,0,0,1,0,1,1,0,0,0,1)$	7,10,14,16	6,9,13,15	2^{-23}
$(0,0,0,0,0,1,1,0,1,1,0,1,0,0,0,0) \xrightarrow{1r} (1,0,1,0,0,0,0,0,0,0,1,0,1,1,1,1)$	7,10,12,17,18	6,9,17,18	2^{-12}
$(0,0,0,0,0,1,1,0,1,1,0,1,0,0,0,1) \xrightarrow{1r} (0,1,0,1,1,1,1,1,1,1,0,1,0,0,0,1)$	7,10,12,16	6,9	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,1,1,0,1,0,0,1,0) \xrightarrow{1r} (0,1,1,0,0,0,0,1,0,0,1,0,1,1,1,1)$	7,10,12,17	6,9,15,17	2^{-12}
$(0,0,0,0,0,1,1,0,1,1,0,1,0,0,1,1) \xrightarrow{1r} (1,0,0,1,1,1,1,0,1,1,0,1,0,0,0,1)$	7,10,12,16,18	6,9,15,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,1,1,0,1,0,1,0,0) \xrightarrow{1r} (0,1,1,1,1,0,1,0,1,0,1,0,1,0,0,0)$	7,10,12,14	6,9	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,1,1,0,1,0,1,0,1) \xrightarrow{1r} (1,0,0,0,0,0,1,0,1,0,1,0,1,1,1,0)$	7,10,12,14,16,17,18	6,9,17,18	2^{-23}
$(0,0,0,0,0,1,1,0,1,1,0,1,0,1,0,1) \xrightarrow{1r} (1,0,1,1,1,1,0,0,0,1,0,1,0,0,0,0)$	7,10,12,14,18	6,9,15,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,1,1,0,1,0,1,1,1) \xrightarrow{1r} (0,1,0,0,0,0,1,1,1,0,1,0,1,1,1,0)$	7,10,12,14,16,17	6,9,15,17	2^{-23}
$(0,0,0,0,0,1,1,0,1,1,0,1,0,1,0,0) \xrightarrow{1r} (0,1,1,1,0,1,0,0,0,1,1,0,1,1,1,1)$	7,10,12,17	6,9,13,17	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,1,1,0,1,0,0,0,1) \xrightarrow{1r} (1,0,0,0,1,0,1,1,1,0,0,1,0,0,0,1)$	7,10,12,16,18	6,9,13,18	2^{-23}
$(0,0,0,0,0,1,1,0,1,1,0,1,0,1,0,1) \xrightarrow{1r} (1,0,1,1,0,1,0,1,0,1,1,0,1,1,1,1)$	7,10,12,17,18	6,9,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,1,1,0,1,0,1,0,1) \xrightarrow{1r} (0,1,0,0,1,0,1,0,1,0,0,1,0,0,0,1)$	7,10,12,16	6,9,13,15	2^{-23}
$(0,0,0,0,0,1,1,0,1,1,0,1,1,1,0,0) \xrightarrow{1r} (1,0,1,0,1,0,0,1,0,0,0,1,0,0,0,0)$	7,10,12,14,18	6,9,13,18	2^{-12}
$(0,0,0,0,0,1,1,0,1,1,0,1,1,1,0,1) \xrightarrow{1r} (0,1,0,1,0,1,1,0,1,1,1,0,1,1,1,0)$	7,10,12,14,16,17	6,9,13,17	$2^{-17.5}$
$(0,0,0,0,0,1,1,0,1,1,0,1,1,1,1,0) \xrightarrow{1r} (0,1,1,0,1,0,0,0,0,0,0,1,0,0,0,0)$	7,10,12,14	6,9,13,15	2^{-12}
$(0,0,0,0,0,1,1,0,1,1,0,1,1,1,1,1) \xrightarrow{1r} (1,0,0,1,0,1,1,1,1,1,1,0,1,1,1,0)$	7,10,12,14,16,17,18	6,9,13,15,17,18	$2^{-17.5}$

Table 0.56 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	7,10,18	6,9,11,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	7,10,16,17	6,9,11,17	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	7,10	6,9,11,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	7,10,16,17,18	6,9,11,15,17,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	7,10,14,17	6,9,11,17	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	7,10,14,16,18	6,9,11,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	7,10,14,17,18	6,9,11,15,17,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	7,10,14,16	6,9,11,15	$2^{-28.5}$
$(0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	7,10	6,9,11,13	2^{-23}
$(0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	7,10,16,17,18	6,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	7,10,18	6,9,11,13,15,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	7,10,16,17	6,9,11,13,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	7,10,14,17,18	6,9,11,13,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	7,10,14,16	6,9,11,13	2^{-23}
$(0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	7,10,14,17	6,9,11,13,15,17	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	7,10,14,16,18	6,9,11,13,15,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	7,10,12,17	6,9,11,17	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	7,10,12,16,18	6,9,11,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	7,10,12,17,18	6,9,11,15,17,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	7,10,12,16	6,9,11,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	7,10,12,14,18	6,9,11,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	7,10,12,14,16,17	6,9,11,17	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	7,10,12,14	6,9,11,15	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	7,10,12,14,16,17,18	6,9,11,15,17,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	7,10,12,17,18	6,9,11,13,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	7,10,12,16	6,9,11,13	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	7,10,12,17	6,9,11,13,15,17	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	7,10,12,16,18	6,9,11,13,15,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	7,10,12,14	6,9,11,13	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	7,10,12,14,16,17,18	6,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	7,10,12,14,18	6,9,11,13,15,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	7,10,12,14,16,17	6,9,11,13,15,17	$2^{-17.5}$

Table 0.57 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(2)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	7,18	6,8,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	7,16,17	6,8,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	7	6,8,15	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	7,16,17,18	6,8,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	7,14,17	6,8,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	7,14,16,18	6,8,18	2^{-1}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	7,14,17,18	6,8,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	7,14,16	6,8,15	2^{-1}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	7	6,8,13	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	7,16,17,18	6,8,13,17,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	7,18	6,8,13,15,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	7,16,17	6,8,13,15,17	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	7,14,17,18	6,8,13,17,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	7,14,16	6,8,13	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	7,14,17	6,8,13,15,17	2^{-23}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	7,14,16,18	6,8,13,15,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	7,12,17	6,8,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	7,12,16,18	6,8,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	7,12,17,18	6,8,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	7,12,16	6,8,15	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	7,12,14,18	6,8,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	7,12,14,16,17	6,8,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	7,12,14	6,8,15	2^{-23}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	7,12,14,16,17,18	6,8,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	7,12,17,18	6,8,13,17,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	7,12,16	6,8,13	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	7,12,17	6,8,13,15,17	2^{-23}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	7,12,16,18	6,8,13,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	7,12,14	6,8,13	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	7,12,14,16,17,18	6,8,13,17,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	7,12,14,18	6,8,13,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	7,12,14,16,17	6,8,13,15,17	2^{-12}

Table 0.58 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	7	6,8,11	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	7,16,17,18	6,8,11,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	7,18	6,8,11,15,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	7,16,17	6,8,11,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	7,14,17,18	6,8,11,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	7,14,16	6,8,11	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	7,14,17	6,8,11,15,17	$2^{-28.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	7,14,16,18	6,8,11,15,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	7,18	6,8,11,13,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	7,16,17	6,8,11,13,17	2^{-23}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	7	6,8,11,13,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	7,16,17,18	6,8,11,13,15,17,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	7,14,17	6,8,11,13,17	2^{-23}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	7,14,16,18	6,8,11,13,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	7,14,17,18	6,8,11,13,15,17,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	7,14,16	6,8,11,13,15	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	7,12,17,18	6,8,11,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	7,12,16	6,8,11	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	7,12,17	6,8,11,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	7,12,16,18	6,8,11,15,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	7,12,14	6,8,11	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	7,12,14,16,17,18	6,8,11,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	7,12,14,18	6,8,11,15,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	7,12,14,16,17	6,8,11,15,17	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	7,12,17	6,8,11,13,17	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	7,12,16,18	6,8,11,13,18	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	7,12,17,18	6,8,11,13,15,17,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	7,12,16	6,8,11,13,15	$2^{-6.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	7,12,14,18	6,8,11,13,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	7,12,14,16,17	6,8,11,13,17	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	7,12,14	6,8,11,13,15	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	7,12,14,16,17,18	6,8,11,13,15,17,18	2^{-12}

Table 0.59 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(2)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	7,10,17	6,8,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	7,10,16,18	6,8,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	7,10,17,18	6,8,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	7,10,16	6,8,15	2^{-23}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	7,10,14,18	6,8,18	2^{-34}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	7,10,14,16,17	6,8,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	7,10,14	6,8,15	2^{-34}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	7,10,14,16,17,18	6,8,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	7,10,17,18	6,8,13,17,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	7,10,16	6,8,13	$2^{-28.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	7,10,17	6,8,13,15,17	2^{-23}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	7,10,16,18	6,8,13,15,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	7,10,14	6,8,13	$2^{-28.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	7,10,14,16,17,18	6,8,13,17,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	7,10,14,18	6,8,13,15,18	$2^{-28.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	7,10,14,16,17	6,8,13,15,17	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	7,10,12,18	6,8,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	7,10,12,16,17	6,8,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	7,10,12	6,8,15	2^{-23}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	7,10,12,16,17,18	6,8,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	7,10,12,14,17	6,8,17	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	7,10,12,14,16,18	6,8,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	7,10,12,14,17,18	6,8,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	7,10,12,14,16	6,8,15	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	7,10,12	6,8,13	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	7,10,12,16,17,18	6,8,13,17,18	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	7,10,12,18	6,8,13,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	7,10,12,16,17	6,8,13,15,17	2^{-12}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	7,10,12,14,17,18	6,8,13,17,18	2^{-23}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	7,10,12,14,16	6,8,13	$2^{-17.5}$
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	7,10,12,14,17	6,8,13,15,17	2^{-23}
$(0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	7,10,12,14,16,18	6,8,13,15,18	$2^{-17.5}$

Table 0.60 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,0,1,1,1,0,1,1,0,0,0,0,0) \xrightarrow{1r} (1,1,0,1,0,0,0,1,1,0,0,0,1,0,0,1)$	7,10,17,18	6,8,11,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,0,1,1,0,0,0,0,1) \xrightarrow{1r} (0,0,1,0,1,1,1,0,0,1,1,1,0,1,1,1)$	7,10,16	6,8,11	2^{-23}
$(0,0,0,0,0,1,1,1,0,1,1,0,0,0,1,0) \xrightarrow{1r} (0,0,0,1,0,0,0,0,1,0,0,0,1,0,0,1)$	7,10,17	6,8,11,15,17	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,0,1,1,0,0,0,1,1) \xrightarrow{1r} (1,1,1,0,1,1,1,1,0,1,1,1,0,1,1,1)$	7,10,16,18	6,8,11,15,18	2^{-23}
$(0,0,0,0,0,1,1,1,0,1,1,0,0,1,0,0) \xrightarrow{1r} (0,0,0,0,1,1,0,0,1,1,1,1,0,1,1,0)$	7,10,14	6,8,11	2^{-23}
$(0,0,0,0,0,1,1,1,0,1,1,0,0,1,0,1) \xrightarrow{1r} (1,1,1,1,0,0,1,1,0,0,0,0,1,0,0,0)$	7,10,14,16,17,18	6,8,11,17,18	$2^{-6.5}$
$(0,0,0,0,0,1,1,1,0,1,1,0,0,1,1,0) \xrightarrow{1r} (1,1,0,0,1,1,0,1,1,1,1,1,0,1,1,0)$	7,10,14,18	6,8,11,15,18	2^{-23}
$(0,0,0,0,0,1,1,1,0,1,1,0,0,1,1,1) \xrightarrow{1r} (0,0,1,1,0,0,1,0,0,0,0,0,1,0,0,0)$	7,10,14,16,17	6,8,11,15,17	$2^{-6.5}$
$(0,0,0,0,0,1,1,1,0,1,1,0,1,0,0,0) \xrightarrow{1r} (0,0,0,0,0,1,0,1,1,1,0,0,1,0,0,1)$	7,10,17	6,8,11,13,17	2^{-12}
$(0,0,0,0,0,1,1,1,0,1,1,0,1,0,0,1) \xrightarrow{1r} (1,1,1,1,1,0,1,0,0,0,1,1,0,1,1,1)$	7,10,16,18	6,8,11,13,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,0,1,1,0,1,0,1,0) \xrightarrow{1r} (1,1,0,0,0,1,0,0,1,1,0,0,1,0,0,1)$	7,10,17,18	6,8,11,13,15,17,18	2^{-12}
$(0,0,0,0,0,1,1,1,0,1,1,0,1,0,1,1) \xrightarrow{1r} (0,0,1,1,1,0,1,1,0,0,1,1,0,1,1,1)$	7,10,16	6,8,11,13,15	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,0,1,1,0,1,1,0,0) \xrightarrow{1r} (1,1,0,1,1,0,0,0,1,0,1,1,0,1,1,0)$	7,10,14,18	6,8,11,13,18	$2^{-28.5}$
$(0,0,0,0,0,1,1,1,0,1,1,0,1,1,0,1) \xrightarrow{1r} (0,0,1,0,0,1,1,1,0,1,0,0,1,0,0,0)$	7,10,14,16,17	6,8,11,13,17	2^{-12}
$(0,0,0,0,0,1,1,1,0,1,1,0,1,1,1,0) \xrightarrow{1r} (0,0,0,1,1,0,0,1,1,0,1,1,0,1,1,0)$	7,10,14	6,8,11,13,15	$2^{-28.5}$
$(0,0,0,0,0,1,1,1,0,1,1,0,1,1,1,1) \xrightarrow{1r} (1,1,1,0,0,1,1,0,0,1,0,0,1,0,0,0)$	7,10,14,16,17,18	6,8,11,13,15,17,18	2^{-12}
$(0,0,0,0,0,1,1,1,0,1,1,1,0,0,0,0) \xrightarrow{1r} (0,0,0,0,1,1,1,0,1,1,0,1,0,1,1,0)$	7,10,12	6,8,11	2^{-23}
$(0,0,0,0,0,1,1,1,0,1,1,1,0,0,0,1) \xrightarrow{1r} (1,1,1,1,0,0,0,1,0,0,1,0,1,0,0,0)$	7,10,12,16,17,18	6,8,11,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,0,1,1,1,0,0,1,0) \xrightarrow{1r} (1,1,0,0,1,1,1,1,1,1,0,1,0,1,1,0)$	7,10,12,18	6,8,11,15,18	2^{-23}
$(0,0,0,0,0,1,1,1,0,1,1,1,0,0,1,1) \xrightarrow{1r} (0,0,1,1,0,0,0,0,0,0,1,0,1,0,0,0)$	7,10,12,16,17	6,8,11,15,17	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,0,1,1,1,0,1,0,0) \xrightarrow{1r} (1,1,0,1,0,0,1,1,1,0,1,0,1,0,0,1)$	7,10,12,14,17,18	6,8,11,17,18	$2^{-28.5}$
$(0,0,0,0,0,1,1,1,0,1,1,1,0,1,0,1) \xrightarrow{1r} (0,0,1,0,1,1,0,0,0,1,0,1,0,1,1,1)$	7,10,12,14,16	6,8,11	2^{-23}
$(0,0,0,0,0,1,1,1,0,1,1,1,0,1,1,0) \xrightarrow{1r} (0,0,0,1,0,0,1,0,1,0,1,0,1,0,0,1)$	7,10,12,14,17	6,8,11,15,17	$2^{-28.5}$
$(0,0,0,0,0,1,1,1,0,1,1,1,0,1,1,1) \xrightarrow{1r} (1,1,1,0,1,1,0,1,0,1,0,1,0,1,1,1)$	7,10,12,14,16,18	6,8,11,15,18	2^{-23}
$(0,0,0,0,0,1,1,1,0,1,1,1,1,0,0,0) \xrightarrow{1r} (1,1,0,1,1,0,1,0,1,0,1,0,0,1,1,0)$	7,10,12,18	6,8,11,13,18	$2^{-28.5}$
$(0,0,0,0,0,1,1,1,0,1,1,1,1,0,0,1) \xrightarrow{1r} (0,0,1,0,0,1,0,1,0,1,1,0,1,0,0,0)$	7,10,12,16,17	6,8,11,13,17	2^{-23}
$(0,0,0,0,0,1,1,1,0,1,1,1,1,0,1,0) \xrightarrow{1r} (0,0,0,1,1,0,1,1,1,0,0,1,0,1,1,0)$	7,10,12	6,8,11,13,15	$2^{-28.5}$
$(0,0,0,0,0,1,1,1,0,1,1,1,1,0,1,1) \xrightarrow{1r} (1,1,1,0,0,1,0,0,0,1,1,0,1,0,0,0)$	7,10,12,16,17,18	6,8,11,13,15,17,18	2^{-23}
$(0,0,0,0,0,1,1,1,0,1,1,1,1,1,0,0) \xrightarrow{1r} (0,0,0,0,0,1,1,1,1,1,1,0,1,0,0,1)$	7,10,12,14,17	6,8,11,13,17	2^{-23}
$(0,0,0,0,0,1,1,1,0,1,1,1,1,1,0,1) \xrightarrow{1r} (1,1,1,1,1,0,0,0,0,0,0,1,0,1,1,1)$	7,10,12,14,16,18	6,8,11,13,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,0,1,1,1,1,1,1,0) \xrightarrow{1r} (1,1,0,0,0,1,1,0,1,1,1,0,1,0,0,1)$	7,10,12,14,17,18	6,8,11,13,15,17,18	2^{-23}
$(0,0,0,0,0,1,1,1,0,1,1,1,1,1,1,1) \xrightarrow{1r} (0,0,1,1,1,0,0,1,0,0,0,1,0,1,1,1)$	7,10,12,14,16	6,8,11,13,15	$2^{-17.5}$

Table 0.61 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,0,1,1,1,1,0,0,0,0,0,0,0) \xrightarrow{1r} (0,1,1,1,0,1,0,1,1,1,0,1,1,0,1,0)$	7	6,8,9	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,0,0,0,0,0,0,1) \xrightarrow{1r} (1,0,0,0,1,0,1,0,0,0,1,0,0,1,0,0)$	7,16,17,18	6,8,9,17,18	2^{-23}
$(0,0,0,0,0,1,1,1,1,0,0,0,0,0,1,0) \xrightarrow{1r} (1,0,1,1,0,1,0,0,1,1,0,1,1,0,1,0)$	7,18	6,8,9,15,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,0,0,0,0,0,1,1) \xrightarrow{1r} (0,1,0,0,1,0,1,1,0,0,1,0,0,1,0,0)$	7,16,17	6,8,9,15,17	2^{-23}
$(0,0,0,0,0,1,1,1,1,0,0,0,0,1,0,0) \xrightarrow{1r} (1,0,1,0,1,0,0,0,1,0,1,0,0,1,0,1)$	7,14,17,18	6,8,9,17,18	2^{-34}
$(0,0,0,0,0,1,1,1,1,0,0,0,0,1,0,1) \xrightarrow{1r} (0,1,0,1,0,1,1,1,0,1,0,1,1,0,1,1)$	7,14,16	6,8,9	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,0,0,0,0,1,1,0) \xrightarrow{1r} (0,1,1,0,1,0,0,1,1,0,1,0,0,1,0,1)$	7,14,17	6,8,9,15,17	2^{-34}
$(0,0,0,0,0,1,1,1,1,0,0,0,0,1,1,1) \xrightarrow{1r} (1,0,0,1,0,1,1,0,0,1,0,1,1,0,1,1)$	7,14,16,18	6,8,9,15,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,0,0,0,1,0,0,0) \xrightarrow{1r} (1,0,1,0,0,0,0,1,1,0,0,1,1,0,1,0)$	7,18	6,8,9,13,18	2^{-23}
$(0,0,0,0,0,1,1,1,1,0,0,0,1,0,0,1) \xrightarrow{1r} (0,1,0,1,1,1,1,0,0,1,1,0,0,1,0,0)$	7,16,17	6,8,9,13,17	$2^{-28.5}$
$(0,0,0,0,0,1,1,1,1,0,0,0,1,0,1,0) \xrightarrow{1r} (0,1,1,0,0,0,0,0,1,0,0,1,1,0,1,0)$	7	6,8,9,13,15	2^{-23}
$(0,0,0,0,0,1,1,1,1,0,0,0,1,0,1,1) \xrightarrow{1r} (1,0,0,1,1,1,1,1,0,1,1,0,0,1,0,0)$	7,16,17,18	6,8,9,13,15,17,18	$2^{-28.5}$
$(0,0,0,0,0,1,1,1,1,0,0,0,1,1,0,0) \xrightarrow{1r} (0,1,1,1,1,1,0,0,1,1,1,0,0,1,0,1)$	7,14,17	6,8,9,13,17	$2^{-28.5}$
$(0,0,0,0,0,1,1,1,1,0,0,0,1,1,0,1) \xrightarrow{1r} (1,0,0,0,0,0,1,1,0,0,0,1,1,0,1,1)$	7,14,16,18	6,8,9,13,18	2^{-12}
$(0,0,0,0,0,1,1,1,1,0,0,0,1,1,1,0) \xrightarrow{1r} (1,0,1,1,1,1,0,1,1,1,1,0,0,1,0,1)$	7,14,17,18	6,8,9,13,15,17,18	$2^{-28.5}$
$(0,0,0,0,0,1,1,1,1,0,0,0,1,1,1,1) \xrightarrow{1r} (0,1,0,0,0,0,1,0,0,0,0,1,1,0,1,1)$	7,14,16	6,8,9,13,15	2^{-12}
$(0,0,0,0,0,1,1,1,1,0,0,1,0,0,0,0) \xrightarrow{1r} (1,0,1,0,1,0,1,0,1,0,0,0,0,1,0,1)$	7,12,17,18	6,8,9,17,18	2^{-23}
$(0,0,0,0,0,1,1,1,1,0,0,1,0,0,0,1) \xrightarrow{1r} (0,1,0,1,0,1,0,1,0,1,1,1,1,0,1,1)$	7,12,16	6,8,9	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,0,0,1,0,0,1,0) \xrightarrow{1r} (0,1,1,0,1,0,1,1,1,0,0,0,0,1,0,1)$	7,12,17	6,8,9,15,17	2^{-23}
$(0,0,0,0,0,1,1,1,1,0,0,1,0,0,1,1) \xrightarrow{1r} (1,0,0,1,0,1,0,0,0,1,1,1,1,0,1,1)$	7,12,16,18	6,8,9,15,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,0,0,1,0,1,0,0) \xrightarrow{1r} (0,1,1,1,0,1,1,1,1,1,1,1,1,0,1,0)$	7,12,14	6,8,9	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,0,0,1,0,1,0,1) \xrightarrow{1r} (1,0,0,0,1,0,0,0,0,0,0,0,0,1,0,0)$	7,12,14,16,17,18	6,8,9,17,18	2^{-12}
$(0,0,0,0,0,1,1,1,1,0,0,1,0,1,1,0) \xrightarrow{1r} (1,0,1,1,0,1,1,0,1,1,1,1,1,0,1,0)$	7,12,14,18	6,8,9,15,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,0,0,1,0,1,1,1) \xrightarrow{1r} (0,1,0,0,1,0,0,1,0,0,0,0,0,1,0,0)$	7,12,14,16,17	6,8,9,15,17	2^{-12}
$(0,0,0,0,0,1,1,1,1,0,0,1,1,0,0,0) \xrightarrow{1r} (0,1,1,1,1,1,1,0,1,1,1,0,0,0,1,0,1)$	7,12,17	6,8,9,13,17	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,0,0,1,1,0,0,1) \xrightarrow{1r} (1,0,0,0,0,0,0,1,0,0,1,1,1,0,1,1)$	7,12,16,18	6,8,9,13,18	2^{-12}
$(0,0,0,0,0,1,1,1,1,0,0,1,1,0,1,0) \xrightarrow{1r} (1,0,1,1,1,1,1,1,1,1,0,0,0,1,0,1)$	7,12,17,18	6,8,9,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,0,0,1,1,0,1,1) \xrightarrow{1r} (0,1,0,0,0,0,0,0,0,0,1,1,1,0,1,1)$	7,12,16	6,8,9,13,15	2^{-12}
$(0,0,0,0,0,1,1,1,1,0,0,1,1,1,0,0) \xrightarrow{1r} (1,0,1,0,0,0,1,1,1,0,1,1,1,0,1,0)$	7,12,14,18	6,8,9,13,18	2^{-23}
$(0,0,0,0,0,1,1,1,1,0,0,1,1,1,0,1) \xrightarrow{1r} (0,1,0,1,1,1,0,0,0,1,0,0,0,1,0,0)$	7,12,14,16,17	6,8,9,13,17	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,0,0,1,1,1,1,0) \xrightarrow{1r} (0,1,1,0,0,0,1,0,1,0,1,1,1,0,1,0)$	7,12,14	6,8,9,13,15	2^{-23}
$(0,0,0,0,0,1,1,1,1,0,0,1,1,1,1,1) \xrightarrow{1r} (1,0,0,1,1,1,0,1,0,1,0,0,0,1,0,0)$	7,12,14,16,17,18	6,8,9,13,15,17,18	$2^{-17.5}$

Table 0.62 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,0,1,1,1,1,0,1,0,0,0,0,0) \xrightarrow{1r} (1,0,1,1,0,0,0,1,1,0,0,0,1,0,1,0)$	7,18	6,8,9,11,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,0,1,0,0,0,0,1) \xrightarrow{1r} (0,1,0,0,1,1,1,0,0,1,1,1,0,1,0,0)$	7,16,17	6,8,9,11,17	2^{-23}
$(0,0,0,0,0,1,1,1,1,0,1,0,0,0,1,0) \xrightarrow{1r} (0,1,1,1,0,0,0,0,1,0,0,0,1,0,1,0)$	7	6,8,9,11,15	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,0,1,0,0,0,1,1) \xrightarrow{1r} (1,0,0,0,1,1,1,1,0,1,1,1,0,1,0,0)$	7,16,17,18	6,8,9,11,15,17,18	2^{-23}
$(0,0,0,0,0,1,1,1,1,0,1,0,0,1,0,0) \xrightarrow{1r} (0,1,1,0,1,1,0,0,1,1,1,1,0,1,0,1)$	7,14,17	6,8,9,11,17	2^{-23}
$(0,0,0,0,0,1,1,1,1,0,1,0,0,1,0,1) \xrightarrow{1r} (1,0,0,1,0,0,1,1,0,0,0,0,1,0,1,1)$	7,14,16,18	6,8,9,11,18	$2^{-6.5}$
$(0,0,0,0,0,1,1,1,1,0,1,0,0,1,1,0) \xrightarrow{1r} (1,0,1,0,1,1,0,1,1,1,1,1,0,1,0,1)$	7,14,17,18	6,8,9,11,15,17,18	2^{-23}
$(0,0,0,0,0,1,1,1,1,0,1,0,0,1,1,1) \xrightarrow{1r} (0,1,0,1,0,0,1,0,0,0,0,0,1,0,1,1)$	7,14,16	6,8,9,11,15	$2^{-6.5}$
$(0,0,0,0,0,1,1,1,1,0,1,0,1,0,0,0) \xrightarrow{1r} (0,1,1,0,0,1,0,1,1,1,0,0,1,0,1,0)$	7	6,8,9,11,13	2^{-12}
$(0,0,0,0,0,1,1,1,1,0,1,0,1,0,0,1) \xrightarrow{1r} (1,0,0,1,1,0,1,0,0,0,1,1,0,1,0,0)$	7,16,17,18	6,8,9,11,13,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,0,1,0,1,0,1,0) \xrightarrow{1r} (1,0,1,0,0,1,0,0,1,1,0,0,1,0,1,0)$	7,18	6,8,9,11,13,15,18	2^{-12}
$(0,0,0,0,0,1,1,1,1,0,1,0,1,0,1,1) \xrightarrow{1r} (0,1,0,1,1,0,1,1,0,0,1,1,0,1,0,0)$	7,16,17	6,8,9,11,13,15,17	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,0,1,0,1,1,0,0) \xrightarrow{1r} (1,0,1,1,1,0,0,0,1,0,1,1,0,1,0,1)$	7,14,17,18	6,8,9,11,13,17,18	$2^{-28.5}$
$(0,0,0,0,0,1,1,1,1,0,1,0,1,1,0,1) \xrightarrow{1r} (0,1,0,0,0,1,1,1,0,1,0,0,1,0,1,1)$	7,14,16	6,8,9,11,13	2^{-12}
$(0,0,0,0,0,1,1,1,1,0,1,0,1,1,1,0) \xrightarrow{1r} (0,1,1,1,1,0,0,1,1,0,1,1,0,1,0,1)$	7,14,17	6,8,9,11,13,15,17	$2^{-28.5}$
$(0,0,0,0,0,1,1,1,1,0,1,0,1,1,1,1) \xrightarrow{1r} (1,0,0,0,0,1,1,0,0,1,0,0,1,0,1,1)$	7,14,16,18	6,8,9,11,13,15,18	2^{-12}
$(0,0,0,0,0,1,1,1,1,0,1,1,0,0,0,0) \xrightarrow{1r} (0,1,1,0,1,1,1,0,1,1,0,1,0,1,0,1)$	7,12,17	6,8,9,11,17	2^{-23}
$(0,0,0,0,0,1,1,1,1,0,1,1,0,0,0,1) \xrightarrow{1r} (1,0,0,1,0,0,0,1,0,0,1,0,1,0,1,1)$	7,12,16,18	6,8,9,11,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,0,1,1,0,0,1,0) \xrightarrow{1r} (1,0,1,0,1,1,1,1,1,1,0,1,0,1,0,1)$	7,12,17,18	6,8,9,11,15,17,18	2^{-23}
$(0,0,0,0,0,1,1,1,1,0,1,1,0,0,1,1) \xrightarrow{1r} (0,1,0,1,0,0,0,0,0,0,1,0,1,0,1,1)$	7,12,16	6,8,9,11,15	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,0,1,1,0,1,0,0) \xrightarrow{1r} (1,0,1,1,0,0,1,1,1,0,1,0,1,0,1,0)$	7,12,14,18	6,8,9,11,18	$2^{-28.5}$
$(0,0,0,0,0,1,1,1,1,0,1,1,0,1,0,1) \xrightarrow{1r} (0,1,0,0,1,1,0,0,0,1,0,1,0,1,0,0)$	7,12,14,16,17	6,8,9,11,17	2^{-23}
$(0,0,0,0,0,1,1,1,1,0,1,1,0,1,1,0) \xrightarrow{1r} (0,1,1,1,0,0,1,0,1,0,1,0,1,0,1,0)$	7,12,14	6,8,9,11,15	$2^{-28.5}$
$(0,0,0,0,0,1,1,1,1,0,1,1,0,1,1,1) \xrightarrow{1r} (1,0,0,0,1,1,0,1,0,1,0,1,0,1,0,0)$	7,12,14,16,17,18	6,8,9,11,15,17,18	2^{-23}
$(0,0,0,0,0,1,1,1,1,0,1,1,0,1,0,0) \xrightarrow{1r} (1,0,1,1,1,0,1,0,1,0,1,0,0,1,0,1)$	7,12,17,18	6,8,9,11,13,17,18	$2^{-28.5}$
$(0,0,0,0,0,1,1,1,1,0,1,1,0,1,0,1) \xrightarrow{1r} (0,1,0,0,0,1,0,1,0,1,1,0,1,0,1,1)$	7,12,16	6,8,9,11,13	2^{-23}
$(0,0,0,0,0,1,1,1,1,0,1,1,0,1,0,1) \xrightarrow{1r} (0,1,1,1,1,0,1,1,1,0,0,1,0,1,0,1)$	7,12,17	6,8,9,11,13,15,17	$2^{-28.5}$
$(0,0,0,0,0,1,1,1,1,0,1,1,0,1,1,1) \xrightarrow{1r} (1,0,0,0,0,1,0,0,0,1,1,0,1,0,1,1)$	7,12,16,18	6,8,9,11,13,15,18	2^{-23}
$(0,0,0,0,0,1,1,1,1,0,1,1,1,1,0,0) \xrightarrow{1r} (0,1,1,0,0,1,1,1,1,1,1,0,1,0,1,0)$	7,12,14	6,8,9,11,13	2^{-23}
$(0,0,0,0,0,1,1,1,1,0,1,1,1,1,0,1) \xrightarrow{1r} (1,0,0,1,1,0,0,0,0,0,0,1,0,1,0,0)$	7,12,14,16,17,18	6,8,9,11,13,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,0,1,1,1,1,1,0) \xrightarrow{1r} (1,0,1,0,0,1,1,0,1,1,1,0,1,0,1,0)$	7,12,14,18	6,8,9,11,13,15,18	2^{-23}
$(0,0,0,0,0,1,1,1,1,0,1,1,1,1,1,1) \xrightarrow{1r} (0,1,0,1,1,0,0,1,0,0,0,1,0,1,0,0)$	7,12,14,16,17	6,8,9,11,13,15,17	$2^{-17.5}$

Table 0.63 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,0,1,1,1,1,0,0,0,0,0,0) \xrightarrow{1r} (1,0,0,0,0,0,0,0,1,0,0,0,1,1,0,1)$	7,10,17,18	6,8,9,17,18	2^{-12}
$(0,0,0,0,0,1,1,1,1,0,0,0,0,0,1) \xrightarrow{1r} (0,1,1,1,1,1,1,0,1,1,1,0,0,1,1)$	7,10,16	6,8,9	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,0,0,0,0,1,0) \xrightarrow{1r} (0,1,0,0,0,0,0,1,1,0,0,0,1,1,0,1)$	7,10,17	6,8,9,15,17	2^{-12}
$(0,0,0,0,0,1,1,1,1,0,0,0,0,1,1) \xrightarrow{1r} (1,0,1,1,1,1,1,0,0,1,1,1,0,0,1,1)$	7,10,16,18	6,8,9,15,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,0,0,0,1,0,0) \xrightarrow{1r} (0,1,0,1,1,1,0,1,1,1,1,1,0,0,1,0)$	7,10,14	6,8,9	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,0,0,0,1,0,1) \xrightarrow{1r} (1,0,1,0,0,0,1,0,0,0,0,0,1,1,0,0)$	7,10,14,16,17,18	6,8,9,17,18	2^{-1}
$(0,0,0,0,0,1,1,1,1,0,0,0,1,1,0) \xrightarrow{1r} (1,0,0,1,1,1,0,0,1,1,1,1,0,0,1,0)$	7,10,14,18	6,8,9,15,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,0,0,0,1,1,1) \xrightarrow{1r} (0,1,1,0,0,0,1,1,0,0,0,0,1,1,0,0)$	7,10,14,16,17	6,8,9,15,17	2^{-1}
$(0,0,0,0,0,1,1,1,1,0,0,0,1,0,0,0) \xrightarrow{1r} (0,1,0,1,0,1,0,0,1,1,0,0,1,1,0,1)$	7,10,17	6,8,9,13,17	$2^{-6.5}$
$(0,0,0,0,0,1,1,1,1,0,0,0,1,0,0,1) \xrightarrow{1r} (1,0,1,0,1,0,1,1,0,0,1,1,0,0,1,1)$	7,10,16,18	6,8,9,13,18	2^{-12}
$(0,0,0,0,0,1,1,1,1,0,0,0,1,0,1,0) \xrightarrow{1r} (1,0,0,1,0,1,0,1,1,1,0,0,1,1,0,1)$	7,10,17,18	6,8,9,13,15,17,18	$2^{-6.5}$
$(0,0,0,0,0,1,1,1,1,0,0,0,1,0,1,1) \xrightarrow{1r} (0,1,1,0,1,0,1,0,0,0,1,1,0,0,1,1)$	7,10,16	6,8,9,13,15	2^{-12}
$(0,0,0,0,0,1,1,1,1,0,0,0,1,1,0,0) \xrightarrow{1r} (1,0,0,0,1,0,0,1,1,0,1,1,0,0,1,0)$	7,10,14,18	6,8,9,13,18	2^{-23}
$(0,0,0,0,0,1,1,1,1,0,0,0,1,1,0,1) \xrightarrow{1r} (0,1,1,1,0,1,1,0,0,1,0,0,1,1,0,0)$	7,10,14,16,17	6,8,9,13,17	$2^{-6.5}$
$(0,0,0,0,0,1,1,1,1,0,0,0,1,1,1,0) \xrightarrow{1r} (0,1,0,0,1,0,0,0,1,0,1,1,0,0,1,0)$	7,10,14	6,8,9,13,15	2^{-23}
$(0,0,0,0,0,1,1,1,1,0,0,0,1,1,1,1) \xrightarrow{1r} (1,0,1,1,0,1,1,1,0,1,0,0,1,1,0,0)$	7,10,14,16,17,18	6,8,9,13,15,17,18	$2^{-6.5}$
$(0,0,0,0,0,1,1,1,1,0,0,0,1,0,0,0) \xrightarrow{1r} (0,1,0,1,1,1,1,1,1,1,0,1,0,0,1,0)$	7,10,12	6,8,9	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,0,0,0,1,0,0,1) \xrightarrow{1r} (1,0,1,0,0,0,0,0,0,0,1,0,1,1,0,0)$	7,10,12,16,17,18	6,8,9,17,18	2^{-12}
$(0,0,0,0,0,1,1,1,1,0,0,0,1,0,1,0) \xrightarrow{1r} (1,0,0,1,1,1,1,0,1,1,0,1,0,0,1,0)$	7,10,12,18	6,8,9,15,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,0,0,0,1,0,1,1) \xrightarrow{1r} (0,1,1,0,0,0,0,1,0,0,1,0,1,1,0,0)$	7,10,12,16,17	6,8,9,15,17	2^{-12}
$(0,0,0,0,0,1,1,1,1,0,0,0,1,0,1,0) \xrightarrow{1r} (1,0,0,0,0,0,1,0,1,0,1,0,1,1,0,1)$	7,10,12,14,17,18	6,8,9,17,18	2^{-23}
$(0,0,0,0,0,1,1,1,1,0,0,0,1,0,1,0) \xrightarrow{1r} (0,1,1,1,1,1,0,1,0,1,0,1,0,0,1,1)$	7,10,12,14,16	6,8,9	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,0,0,0,1,0,1,1) \xrightarrow{1r} (0,1,0,0,0,0,1,1,1,0,1,0,1,1,0,1)$	7,10,12,14,17	6,8,9,15,17	2^{-23}
$(0,0,0,0,0,1,1,1,1,0,0,0,1,0,1,1) \xrightarrow{1r} (1,0,1,1,1,1,0,0,0,1,0,1,0,0,1,1)$	7,10,12,14,16,18	6,8,9,15,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,0,0,0,1,0,1,0) \xrightarrow{1r} (1,0,0,0,1,0,1,1,1,0,0,1,0,0,1,0)$	7,10,12,18	6,8,9,13,18	2^{-23}
$(0,0,0,0,0,1,1,1,1,0,0,0,1,0,1,0) \xrightarrow{1r} (0,1,1,1,0,1,0,0,0,1,1,0,1,1,0,0)$	7,10,12,16,17	6,8,9,13,17	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,0,0,0,1,0,1,0) \xrightarrow{1r} (0,1,0,0,1,0,1,0,1,0,0,1,0,0,1,0)$	7,10,12	6,8,9,13,15	2^{-23}
$(0,0,0,0,0,1,1,1,1,0,0,0,1,0,1,1) \xrightarrow{1r} (1,0,1,1,0,1,0,1,0,1,1,0,1,1,0,0)$	7,10,12,16,17,18	6,8,9,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,0,0,0,1,0,1,1) \xrightarrow{1r} (0,1,0,1,0,1,1,0,1,1,1,0,1,1,0,1)$	7,10,12,14,17	6,8,9,13,17	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,0,0,0,1,0,1,0) \xrightarrow{1r} (1,0,1,0,1,0,0,1,0,0,0,1,0,0,1,1)$	7,10,12,14,16,18	6,8,9,13,18	2^{-12}
$(0,0,0,0,0,1,1,1,1,0,0,0,1,0,1,1) \xrightarrow{1r} (1,0,0,1,0,1,1,1,1,1,0,1,1,0,1,0)$	7,10,12,14,17,18	6,8,9,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,0,0,0,1,0,1,1) \xrightarrow{1r} (0,1,1,0,1,0,0,0,0,0,0,1,0,0,1,1)$	7,10,12,14,16	6,8,9,13,15	2^{-12}

Table 0.64 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,0,1,1,1,1,1,0,0,0,0,0) \xrightarrow{1r} (0,1,0,0,0,1,0,0,1,1,0,1,1,1,0,1)$	7,10,17	6,8,9,11,17	2^{-12}
$(0,0,0,0,0,1,1,1,1,1,0,0,0,0,1) \xrightarrow{1r} (1,0,1,1,1,0,1,1,0,0,1,0,0,0,1,1)$	7,10,16,18	6,8,9,11,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,1,1,0,0,0,1,0) \xrightarrow{1r} (1,0,0,0,0,1,0,1,1,1,0,1,1,1,0,1)$	7,10,17,18	6,8,9,11,15,17,18	2^{-12}
$(0,0,0,0,0,1,1,1,1,1,1,0,0,0,1,1) \xrightarrow{1r} (0,1,1,1,1,0,1,0,0,0,1,0,0,0,1,1)$	7,10,16	6,8,9,11,15	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,1,1,0,0,1,0,0) \xrightarrow{1r} (1,0,0,1,1,0,0,1,1,0,1,0,0,0,1,0)$	7,10,14,18	6,8,9,11,18	$2^{-28.5}$
$(0,0,0,0,0,1,1,1,1,1,1,0,0,1,0,1) \xrightarrow{1r} (0,1,1,0,0,1,1,0,0,1,0,1,1,1,0,0)$	7,10,14,16,17	6,8,9,11,17	2^{-12}
$(0,0,0,0,0,1,1,1,1,1,1,0,0,1,1,0) \xrightarrow{1r} (0,1,0,1,1,0,0,0,1,0,1,0,0,0,1,0)$	7,10,14	6,8,9,11,15	$2^{-28.5}$
$(0,0,0,0,0,1,1,1,1,1,1,0,0,1,1,1) \xrightarrow{1r} (1,0,1,0,0,1,1,1,0,1,0,1,1,1,0,0)$	7,10,14,16,17,18	6,8,9,11,15,17,18	2^{-12}
$(0,0,0,0,0,1,1,1,1,1,1,0,1,0,0,0) \xrightarrow{1r} (1,0,0,1,0,0,0,0,1,0,0,1,1,1,0,1)$	7,10,17,18	6,8,9,11,13,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,1,1,0,1,0,0,1) \xrightarrow{1r} (0,1,1,0,1,1,1,1,0,1,1,0,0,0,1,1)$	7,10,16	6,8,9,11,13	2^{-23}
$(0,0,0,0,0,1,1,1,1,1,1,0,1,0,1,0) \xrightarrow{1r} (0,1,0,1,0,0,0,1,1,0,0,1,1,1,0,1)$	7,10,17	6,8,9,11,13,15,17	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,1,1,0,1,0,1,1) \xrightarrow{1r} (1,0,1,0,1,1,1,1,0,0,1,1,0,0,0,1,1)$	7,10,16,18	6,8,9,11,13,15,18	2^{-23}
$(0,0,0,0,0,1,1,1,1,1,1,0,1,1,0,0) \xrightarrow{1r} (0,1,0,0,1,1,0,1,1,1,1,0,0,0,1,0)$	7,10,14	6,8,9,11,13	2^{-23}
$(0,0,0,0,0,1,1,1,1,1,1,0,1,1,0,1) \xrightarrow{1r} (1,0,1,1,0,0,1,0,0,0,0,1,1,1,0,0)$	7,10,14,16,17,18	6,8,9,11,13,17,18	$2^{-6.5}$
$(0,0,0,0,0,1,1,1,1,1,1,0,1,1,1,0) \xrightarrow{1r} (1,0,0,0,1,1,0,0,1,1,1,0,0,0,1,0)$	7,10,14,18	6,8,9,11,13,15,18	2^{-23}
$(0,0,0,0,0,1,1,1,1,1,1,0,1,1,1,1) \xrightarrow{1r} (0,1,1,1,0,0,1,1,0,0,0,1,1,1,0,0)$	7,10,14,16,17	6,8,9,11,13,15,17	$2^{-6.5}$
$(0,0,0,0,0,1,1,1,1,1,1,1,0,0,0,0) \xrightarrow{1r} (1,0,0,1,1,0,1,1,1,0,0,0,0,0,1,0)$	7,10,12,18	6,8,9,11,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,1,1,1,0,0,0,1) \xrightarrow{1r} (0,1,1,0,0,1,0,0,0,1,1,1,1,1,0,0)$	7,10,12,16,17	6,8,9,11,17	2^{-12}
$(0,0,0,0,0,1,1,1,1,1,1,1,0,0,1,0) \xrightarrow{1r} (0,1,0,1,1,0,1,0,1,0,1,0,0,0,0,1,0)$	7,10,12	6,8,9,11,15	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,1,1,1,0,0,1,1) \xrightarrow{1r} (1,0,1,0,0,1,0,1,0,1,1,1,1,1,0,0)$	7,10,12,16,17,18	6,8,9,11,15,17,18	2^{-12}
$(0,0,0,0,0,1,1,1,1,1,1,1,0,1,0,0) \xrightarrow{1r} (0,1,0,0,0,1,1,0,1,1,1,1,1,1,0,1)$	7,10,12,14,17	6,8,9,11,17	2^{-12}
$(0,0,0,0,0,1,1,1,1,1,1,1,0,1,0,1) \xrightarrow{1r} (1,0,1,1,1,0,0,1,0,0,0,0,0,0,1,1)$	7,10,12,14,16,18	6,8,9,11,18	$2^{-6.5}$
$(0,0,0,0,0,1,1,1,1,1,1,1,0,1,1,0) \xrightarrow{1r} (1,0,0,0,0,1,1,1,1,1,1,1,1,1,0,1)$	7,10,12,14,17,18	6,8,9,11,15,17,18	2^{-12}
$(0,0,0,0,0,1,1,1,1,1,1,1,0,1,1,1) \xrightarrow{1r} (0,1,1,1,1,0,0,0,0,0,0,0,0,0,0,1,1)$	7,10,12,14,16	6,8,9,11,15	$2^{-6.5}$
$(0,0,0,0,0,1,1,1,1,1,1,1,1,0,0,0) \xrightarrow{1r} (0,1,0,0,1,1,1,1,1,1,0,0,0,0,1,0)$	7,10,12	6,8,9,11,13	2^{-12}
$(0,0,0,0,0,1,1,1,1,1,1,1,1,0,0,1) \xrightarrow{1r} (1,0,1,1,0,0,0,0,0,0,0,1,1,1,1,0,0)$	7,10,12,16,17,18	6,8,9,11,13,17,18	$2^{-6.5}$
$(0,0,0,0,0,1,1,1,1,1,1,1,1,0,1,0) \xrightarrow{1r} (1,0,0,0,1,1,1,0,1,1,0,0,0,0,1,0)$	7,10,12,18	6,8,9,11,13,15,18	2^{-12}
$(0,0,0,0,0,1,1,1,1,1,1,1,1,0,1,1) \xrightarrow{1r} (0,1,1,1,0,0,0,1,0,0,1,1,1,1,0,0)$	7,10,12,16,17	6,8,9,11,13,15,17	$2^{-6.5}$
$(0,0,0,0,0,1,1,1,1,1,1,1,1,1,0,0) \xrightarrow{1r} (1,0,0,1,0,0,1,0,1,0,1,1,1,1,0,1)$	7,10,12,14,17,18	6,8,9,11,13,17,18	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,1,1,1,1,1,0,1) \xrightarrow{1r} (0,1,1,0,1,1,0,1,0,1,0,0,0,0,1,1)$	7,10,12,14,16	6,8,9,11,13	2^{-12}
$(0,0,0,0,0,1,1,1,1,1,1,1,1,1,1,0) \xrightarrow{1r} (0,1,0,1,0,0,1,1,1,0,1,1,1,1,0,1)$	7,10,12,14,17	6,8,9,11,13,15,17	$2^{-17.5}$
$(0,0,0,0,0,1,1,1,1,1,1,1,1,1,1,1) \xrightarrow{1r} (1,0,1,0,1,1,0,0,0,1,0,0,0,0,1,1)$	7,10,12,14,16,18	6,8,9,11,13,15,18	2^{-12}

Table 0.65 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (1,1,0,1,0,0,0,0,0,1,0,1,0,0,0,0)$	5,18	18	$2^{-6.5}$
$(0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,1) \xrightarrow{1r} (0,0,1,0,1,1,1,1,1,0,1,0,1,1,1,0)$	5,16,17	17	2^{-23}
$(0,0,0,0,1,0,0,0,0,0,0,0,0,0,1,0) \xrightarrow{1r} (0,0,0,1,0,0,0,1,0,1,0,1,0,0,0,0)$	5	15	$2^{-6.5}$
$(0,0,0,0,1,0,0,0,0,0,0,0,0,0,1,1) \xrightarrow{1r} (1,1,1,0,1,1,1,0,1,0,1,0,1,1,1,0)$	5,16,17,18	15,17,18	2^{-23}
$(0,0,0,0,1,0,0,0,0,0,0,0,0,1,0,0) \xrightarrow{1r} (0,0,0,0,1,1,0,1,0,0,1,0,1,1,1,1)$	5,14,17	17	2^{-12}
$(0,0,0,0,1,0,0,0,0,0,0,0,0,1,0,1) \xrightarrow{1r} (1,1,1,1,0,0,1,0,1,1,0,1,0,0,0,1)$	5,14,16,18	18	$2^{-6.5}$
$(0,0,0,0,1,0,0,0,0,0,0,0,0,1,1,0) \xrightarrow{1r} (1,1,0,0,1,1,0,0,0,0,1,0,1,1,1,1)$	5,14,17,18	15,17,18	2^{-12}
$(0,0,0,0,1,0,0,0,0,0,0,0,0,1,1,1) \xrightarrow{1r} (0,0,1,1,0,0,1,1,1,1,0,1,0,0,0,1)$	5,14,16	15	$2^{-6.5}$
$(0,0,0,0,1,0,0,0,0,0,0,0,0,1,0,0) \xrightarrow{1r} (0,0,0,0,0,1,0,0,0,0,0,1,0,0,0,0)$	5	13	2^{-1}
$(0,0,0,0,1,0,0,0,0,0,0,0,0,1,0,1) \xrightarrow{1r} (1,1,1,1,1,0,1,1,1,1,1,0,1,1,1,0)$	5,16,17,18	13,17,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,0,0,0,0,0,0,1,0,1) \xrightarrow{1r} (1,1,0,0,0,1,0,1,0,0,0,1,0,0,0,0)$	5,18	13,15,18	2^{-1}
$(0,0,0,0,1,0,0,0,0,0,0,0,0,1,0,1) \xrightarrow{1r} (0,0,1,1,1,0,1,0,1,1,1,0,1,1,1,0)$	5,16,17	13,15,17	$2^{-17.5}$
$(0,0,0,0,1,0,0,0,0,0,0,0,0,1,1,0) \xrightarrow{1r} (1,1,0,1,1,0,0,1,0,1,1,0,1,1,1,1)$	5,14,17,18	13,17,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,0,0,0,0,0,0,1,1,0) \xrightarrow{1r} (0,0,1,0,0,1,1,0,1,0,0,1,0,0,0,1)$	5,14,16	13	2^{-12}
$(0,0,0,0,1,0,0,0,0,0,0,0,0,1,1,1) \xrightarrow{1r} (0,0,0,1,1,0,0,0,0,1,1,0,1,1,1,1)$	5,14,17	13,15,17	$2^{-17.5}$
$(0,0,0,0,1,0,0,0,0,0,0,0,0,1,1,1) \xrightarrow{1r} (1,1,1,0,0,1,1,1,1,0,0,1,0,0,0,1)$	5,14,16,18	13,15,18	2^{-12}
$(0,0,0,0,1,0,0,0,0,0,0,0,1,0,0,0) \xrightarrow{1r} (0,0,0,0,1,1,1,1,0,0,0,0,1,1,1,1)$	5,12,17	17	2^{-12}
$(0,0,0,0,1,0,0,0,0,0,0,0,1,0,0,0) \xrightarrow{1r} (1,1,1,1,0,0,0,0,1,1,1,1,0,0,0,1)$	5,12,16,18	18	$2^{-17.5}$
$(0,0,0,0,1,0,0,0,0,0,0,0,1,0,0,1) \xrightarrow{1r} (1,1,0,0,1,1,1,0,0,0,0,0,1,1,1,1)$	5,12,17,18	15,17,18	2^{-12}
$(0,0,0,0,1,0,0,0,0,0,0,0,1,0,0,1) \xrightarrow{1r} (0,0,1,1,0,0,0,1,1,1,1,1,0,0,0,1)$	5,12,16	15	$2^{-17.5}$
$(0,0,0,0,1,0,0,0,0,0,0,0,1,0,1,0) \xrightarrow{1r} (1,1,0,1,0,0,1,0,0,1,1,1,0,0,0,0)$	5,12,14,18	18	$2^{-17.5}$
$(0,0,0,0,1,0,0,0,0,0,0,0,1,0,1,0) \xrightarrow{1r} (0,0,1,0,1,1,0,1,1,0,0,0,1,1,1,0)$	5,12,14,16,17	17	2^{-23}
$(0,0,0,0,1,0,0,0,0,0,0,0,1,0,1,1) \xrightarrow{1r} (0,0,0,1,0,0,1,1,0,1,1,1,0,0,0,0)$	5,12,14	15	$2^{-17.5}$
$(0,0,0,0,1,0,0,0,0,0,0,0,1,0,1,1) \xrightarrow{1r} (1,1,1,0,1,1,0,0,1,0,0,0,1,1,1,0)$	5,12,14,16,17,18	15,17,18	2^{-23}
$(0,0,0,0,1,0,0,0,0,0,0,0,1,1,0,0) \xrightarrow{1r} (1,1,0,1,1,0,1,1,0,1,0,0,1,1,1,1)$	5,12,17,18	13,17,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,0,0,0,0,0,1,1,0,0) \xrightarrow{1r} (0,0,1,0,0,1,0,0,1,0,1,1,0,0,0,1)$	5,12,16	13	2^{-23}
$(0,0,0,0,1,0,0,0,0,0,0,0,1,1,0,1) \xrightarrow{1r} (0,0,0,1,1,0,1,0,0,1,0,0,1,1,1,1)$	5,12,17	13,15,17	$2^{-17.5}$
$(0,0,0,0,1,0,0,0,0,0,0,0,1,1,0,1) \xrightarrow{1r} (1,1,1,0,0,1,0,1,1,0,1,1,0,0,0,1)$	5,12,16,18	13,15,18	2^{-23}
$(0,0,0,0,1,0,0,0,0,0,0,0,1,1,1,0) \xrightarrow{1r} (0,0,0,0,0,1,1,0,0,0,1,1,0,0,0,0)$	5,12,14	13	2^{-12}
$(0,0,0,0,1,0,0,0,0,0,0,0,1,1,1,0) \xrightarrow{1r} (1,1,1,1,1,0,0,1,1,1,0,0,1,1,1,0)$	5,12,14,16,17,18	13,17,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,0,0,0,0,0,1,1,1,0) \xrightarrow{1r} (1,1,0,0,0,1,1,1,0,0,1,1,0,0,0,0)$	5,12,14,18	13,15,18	2^{-12}
$(0,0,0,0,1,0,0,0,0,0,0,0,1,1,1,1) \xrightarrow{1r} (0,0,1,1,1,0,0,0,1,1,0,0,1,1,1,0)$	5,12,14,16,17	13,15,17	$2^{-17.5}$

Table 0.66 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	5	11	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	5,16,17,18	11,17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	5,18	11,15,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	5,16,17	11,15,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	5,14,17,18	11,17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	5,14,16	11	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	5,14,17	11,15,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	5,14,16,18	11,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	5,18	11,13,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	5,16,17	11,13,17	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	5	11,13,15	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	5,16,17,18	11,13,15,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	5,14,17	11,13,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	5,14,16,18	11,13,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	5,14,17,18	11,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	5,14,16	11,13,15	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	5,12,17,18	11,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	5,12,16	11	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	5,12,17	11,15,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	5,12,16,18	11,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	5,12,14	11	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	5,12,14,16,17,18	11,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	5,12,14,18	11,15,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	5,12,14,16,17	11,15,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	5,12,17	11,13,17	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	5,12,16,18	11,13,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	5,12,17,18	11,13,15,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	5,12,16	11,13,15	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	5,12,14,18	11,13,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	5,12,14,16,17	11,13,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	5,12,14	11,13,15	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	5,12,14,16,17,18	11,13,15,17,18	$2^{-17.5}$

Table 0.67 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,0,0,0,0,1,0,0,0,0,0,0) \xrightarrow{1r} (0,0,1,0,0,1,0,1,0,0,0,0,0,1,1,1)$	5,10,17	17	2^{-12}
$(0,0,0,0,1,0,0,0,0,1,0,0,0,0,0,1) \xrightarrow{1r} (1,1,0,1,1,0,1,0,1,1,1,1,1,0,0,1)$	5,10,16,18	18	$2^{-28.5}$
$(0,0,0,0,1,0,0,0,0,1,0,0,0,0,1,0) \xrightarrow{1r} (1,1,1,0,0,1,0,0,0,0,0,0,0,0,1,1)$	5,10,17,18	15,17,18	2^{-12}
$(0,0,0,0,1,0,0,0,0,1,0,0,0,0,1,1) \xrightarrow{1r} (0,0,0,1,1,0,1,1,1,1,1,1,1,0,0,1)$	5,10,16	15	$2^{-28.5}$
$(0,0,0,0,1,0,0,0,0,1,0,0,0,1,0,0) \xrightarrow{1r} (1,1,1,1,1,0,0,0,0,1,1,1,1,0,0,0)$	5,10,14,18	18	$2^{-28.5}$
$(0,0,0,0,1,0,0,0,0,1,0,0,0,1,0,1) \xrightarrow{1r} (0,0,0,0,0,1,1,1,1,0,0,0,0,1,1,0)$	5,10,14,16,17	17	2^{-23}
$(0,0,0,0,1,0,0,0,0,1,0,0,0,1,1,0) \xrightarrow{1r} (0,0,1,1,1,0,0,1,0,1,1,1,1,0,0,0)$	5,10,14	15	$2^{-28.5}$
$(0,0,0,0,1,0,0,0,0,1,0,0,0,1,1,1) \xrightarrow{1r} (1,1,0,0,0,1,1,0,1,0,0,0,0,1,1,0)$	5,10,14,16,17,18	15,17,18	2^{-23}
$(0,0,0,0,1,0,0,0,0,1,0,0,1,0,0,0) \xrightarrow{1r} (1,1,1,1,0,0,0,1,0,1,0,0,0,1,1,1)$	5,10,17,18	13,17,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,0,0,1,0,0,1,0,0,1) \xrightarrow{1r} (0,0,0,0,1,1,1,0,1,0,1,1,1,0,0,1)$	5,10,16	13	2^{-34}
$(0,0,0,0,1,0,0,0,0,1,0,0,1,0,1,0) \xrightarrow{1r} (0,0,1,1,0,0,0,0,0,1,0,0,0,1,1,1)$	5,10,17	13,15,17	$2^{-17.5}$
$(0,0,0,0,1,0,0,0,0,1,0,0,1,0,1,1) \xrightarrow{1r} (1,1,0,0,1,1,1,1,1,0,1,1,1,0,0,1)$	5,10,16,18	13,15,18	2^{-34}
$(0,0,0,0,1,0,0,0,0,1,0,0,1,1,0,0) \xrightarrow{1r} (0,0,1,0,1,1,0,0,0,0,1,1,1,0,0,0)$	5,10,14	13	2^{-23}
$(0,0,0,0,1,0,0,0,0,1,0,0,1,1,0,1) \xrightarrow{1r} (1,1,0,1,0,0,1,1,1,1,0,0,0,1,1,0)$	5,10,14,16,17,18	13,17,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,0,0,1,0,0,1,1,1,0) \xrightarrow{1r} (1,1,1,0,1,1,0,1,0,0,1,1,1,0,0,0)$	5,10,14,18	13,15,18	2^{-23}
$(0,0,0,0,1,0,0,0,0,1,0,0,1,1,1,1) \xrightarrow{1r} (0,0,0,1,0,0,1,0,1,1,0,0,0,1,1,0)$	5,10,14,16,17	13,15,17	$2^{-17.5}$
$(0,0,0,0,1,0,0,0,0,1,0,1,0,0,0,0) \xrightarrow{1r} (1,1,1,1,1,0,1,0,0,1,0,1,1,0,0,0)$	5,10,12,18	18	$2^{-17.5}$
$(0,0,0,0,1,0,0,0,0,1,0,1,0,0,0,1) \xrightarrow{1r} (0,0,0,0,0,1,0,1,1,0,1,0,0,1,1,0)$	5,10,12,16,17	17	2^{-23}
$(0,0,0,0,1,0,0,0,0,1,0,1,0,0,1,0) \xrightarrow{1r} (0,0,1,1,1,0,1,1,0,1,0,1,1,0,0,0)$	5,10,12	15	$2^{-17.5}$
$(0,0,0,0,1,0,0,0,0,1,0,1,0,0,1,1) \xrightarrow{1r} (1,1,0,0,0,1,0,0,1,0,1,0,0,1,1,0)$	5,10,12,16,17,18	15,17,18	2^{-23}
$(0,0,0,0,1,0,0,0,0,1,0,1,0,1,0,0) \xrightarrow{1r} (0,0,1,0,0,1,1,1,0,0,1,0,0,1,1,1)$	5,10,12,14,17	17	2^{-12}
$(0,0,0,0,1,0,0,0,0,1,0,1,0,1,0,1) \xrightarrow{1r} (1,1,0,1,1,0,0,0,1,1,0,1,1,0,0,1)$	5,10,12,14,16,18	18	$2^{-17.5}$
$(0,0,0,0,1,0,0,0,0,1,0,1,0,1,1,0) \xrightarrow{1r} (1,1,1,0,0,1,1,0,0,0,1,0,0,1,1,1)$	5,10,12,14,17,18	15,17,18	2^{-12}
$(0,0,0,0,1,0,0,0,0,1,0,1,0,1,1,1) \xrightarrow{1r} (0,0,0,1,1,0,0,1,1,1,0,1,1,0,0,1)$	5,10,12,14,16	15	$2^{-17.5}$
$(0,0,0,0,1,0,0,0,0,1,0,1,1,0,0,0) \xrightarrow{1r} (0,0,1,0,1,1,1,0,0,0,0,1,1,0,0,0)$	5,10,12	13	2^{-12}
$(0,0,0,0,1,0,0,0,0,1,0,1,1,0,0,1) \xrightarrow{1r} (1,1,0,1,0,0,0,1,1,1,1,0,0,1,1,0)$	5,10,12,16,17,18	13,17,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,0,0,1,0,1,1,0,1,0) \xrightarrow{1r} (1,1,1,0,1,1,1,1,0,0,0,1,1,0,0,0)$	5,10,12,18	13,15,18	2^{-12}
$(0,0,0,0,1,0,0,0,0,1,0,1,1,0,1,1) \xrightarrow{1r} (0,0,0,1,0,0,0,0,1,1,1,0,0,1,1,0)$	5,10,12,16,17	13,15,17	$2^{-17.5}$
$(0,0,0,0,1,0,0,0,0,1,0,1,1,1,0,0) \xrightarrow{1r} (1,1,1,1,0,0,1,1,0,1,1,0,0,1,1,1)$	5,10,12,14,17,18	13,17,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,0,0,1,0,1,1,1,0,1) \xrightarrow{1r} (0,0,0,0,1,1,0,0,1,0,0,1,1,0,0,1)$	5,10,12,14,16	13	2^{-23}
$(0,0,0,0,1,0,0,0,0,1,0,1,1,1,1,0) \xrightarrow{1r} (0,0,1,1,0,0,1,0,0,1,1,0,0,1,1,1)$	5,10,12,14,17	13,15,17	$2^{-17.5}$
$(0,0,0,0,1,0,0,0,0,1,0,1,1,1,1,1) \xrightarrow{1r} (1,1,0,0,1,1,0,1,1,0,0,1,1,0,0,1)$	5,10,12,14,16,18	13,15,18	2^{-23}

Table 0.68 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	5,10,17,18	11,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	5,10,16	11	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	5,10,17	11,15,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	5,10,16,18	11,15,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	5,10,14	11	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	5,10,14,16,17,18	11,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	5,10,14,18	11,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	5,10,14,16,17	11,15,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	5,10,17	11,13,17	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	5,10,16,18	11,13,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	5,10,17,18	11,13,15,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	5,10,16	11,13,15	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	5,10,14,18	11,13,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	5,10,14,16,17	11,13,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	5,10,14	11,13,15	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	5,10,14,16,17,18	11,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	5,10,12	11	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	5,10,12,16,17,18	11,17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	5,10,12,18	11,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	5,10,12,16,17	11,15,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	5,10,12,14,17,18	11,17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	5,10,12,14,16	11	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	5,10,12,14,17	11,15,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	5,10,12,14,16,18	11,15,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	5,10,12,18	11,13,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	5,10,12,16,17	11,13,17	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	5,10,12	11,13,15	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	5,10,12,16,17,18	11,13,15,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	5,10,12,14,17	11,13,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	5,10,12,14,16,18	11,13,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	5,10,12,14,17,18	11,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	5,10,12,14,16	11,13,15	2^{-23}

Table 0.69 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	5	9	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	5,16,17,18	9,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	5,18	9,15,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	5,16,17	9,15,17	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	5,14,17,18	9,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	5,14,16	9	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	5,14,17	9,15,17	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	5,14,16,18	9,15,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	5,18	9,13,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	5,16,17	9,13,17	2^{-34}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	5	9,13,15	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	5,16,17,18	9,13,15,17,18	2^{-34}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	5,14,17	9,13,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	5,14,16,18	9,13,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	5,14,17,18	9,13,15,17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	5,14,16	9,13,15	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	5,12,17,18	9,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	5,12,16	9	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	5,12,17	9,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	5,12,16,18	9,15,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	5,12,14	9	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	5,12,14,16,17,18	9,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	5,12,14,18	9,15,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	5,12,14,16,17	9,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	5,12,17	9,13,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	5,12,16,18	9,13,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	5,12,17,18	9,13,15,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	5,12,16	9,13,15	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	5,12,14,18	9,13,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	5,12,14,16,17	9,13,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	5,12,14	9,13,15	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	5,12,14,16,17,18	9,13,15,17,18	2^{-23}

Table 0.70 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	5,18	9,11,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	5,16,17	9,11,17	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	5	9,11,15	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	5,16,17,18	9,11,15,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	5,14,17	9,11,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	5,14,16,18	9,11,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	5,14,17,18	9,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	5,14,16	9,11,15	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	5	9,11,13	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	5,16,17,18	9,11,13,17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	5,18	9,11,13,15,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	5,16,17	9,11,13,15,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	5,14,17,18	9,11,13,17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	5,14,16	9,11,13	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	5,14,17	9,11,13,15,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	5,14,16,18	9,11,13,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	5,12,17	9,11,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	5,12,16,18	9,11,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	5,12,17,18	9,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	5,12,16	9,11,15	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	5,12,14,18	9,11,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	5,12,17,18	9,11,15,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	5,12,14,16,17	9,11,17	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	5,12,14	9,11,15	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	5,12,14,16,17,18	9,11,15,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	5,12,17,18	9,11,13,17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	5,12,16	9,11,13	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	5,12,17	9,11,13,15,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	5,12,16,18	9,11,13,15,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	5,12,14	9,11,13	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	5,12,14,16,17,18	9,11,13,17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	5,12,14,18	9,11,13,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	5,12,14,16,17	9,11,13,15,17	2^{-23}

Table 0.71 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,0,0,0,1,1,0,0,0,0,0,0) \xrightarrow{1r} (1,0,1,1,0,0,0,0,0,1,0,1,0,0,1,1)$	5,10,17,18	9,17,18	$2^{-6.5}$
$(0,0,0,0,1,0,0,0,1,1,0,0,0,0,0,1) \xrightarrow{1r} (0,1,0,0,1,1,1,1,1,0,1,0,1,1,0,1)$	5,10,16	9	2^{-23}
$(0,0,0,0,1,0,0,0,1,1,0,0,0,0,1,0) \xrightarrow{1r} (0,1,1,1,0,0,0,1,0,1,0,1,0,0,1,1)$	5,10,17	9,15,17	$2^{-6.5}$
$(0,0,0,0,1,0,0,0,1,1,0,0,0,0,1,1) \xrightarrow{1r} (1,0,0,0,1,1,1,0,1,0,1,0,1,1,0,1)$	5,10,16,18	9,15,18	2^{-23}
$(0,0,0,0,1,0,0,0,1,1,0,0,0,1,0,0) \xrightarrow{1r} (0,1,1,0,1,1,0,1,0,0,1,0,1,1,0,0)$	5,10,14	9	2^{-12}
$(0,0,0,0,1,0,0,0,1,1,0,0,0,1,0,1) \xrightarrow{1r} (1,0,0,1,0,0,1,0,1,1,0,1,0,0,1,0)$	5,10,14,16,17,18	9,17,18	$2^{-6.5}$
$(0,0,0,0,1,0,0,0,1,1,0,0,0,1,1,0) \xrightarrow{1r} (1,0,1,0,1,1,0,0,0,0,1,0,1,1,0,0)$	5,10,14,18	9,15,18	2^{-12}
$(0,0,0,0,1,0,0,0,1,1,0,0,0,1,1,1) \xrightarrow{1r} (0,1,0,1,0,0,1,1,1,1,0,1,0,0,1,0)$	5,10,14,16,17	9,15,17	$2^{-6.5}$
$(0,0,0,0,1,0,0,0,1,1,0,0,1,0,0,0) \xrightarrow{1r} (0,1,1,0,0,1,0,0,0,0,0,1,0,0,1,1)$	5,10,17	9,13,17	2^{-1}
$(0,0,0,0,1,0,0,0,1,1,0,0,1,0,0,1) \xrightarrow{1r} (1,0,0,1,1,0,1,1,1,1,0,1,1,0,1)$	5,10,16,18	9,13,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,0,1,1,0,0,1,0,1,0) \xrightarrow{1r} (1,0,1,0,0,1,0,1,0,0,0,1,0,0,1,1)$	5,10,17,18	9,13,15,17,18	2^{-1}
$(0,0,0,0,1,0,0,0,1,1,0,0,1,0,1,1) \xrightarrow{1r} (0,1,0,1,1,0,1,0,1,1,1,0,1,1,0,1)$	5,10,16	9,13,15	$2^{-17.5}$
$(0,0,0,0,1,0,0,0,1,1,0,0,1,1,0,0) \xrightarrow{1r} (1,0,1,1,1,0,0,1,0,1,1,0,1,1,0,0)$	5,10,14,18	9,13,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,0,1,1,0,0,1,1,0,1) \xrightarrow{1r} (0,1,0,0,0,1,1,0,1,0,0,1,0,0,1,0)$	5,10,14,16,17	9,13,17	2^{-12}
$(0,0,0,0,1,0,0,0,1,1,0,0,1,1,1,0) \xrightarrow{1r} (0,1,1,1,1,0,0,0,0,1,1,0,1,1,0,0)$	5,10,14	9,13,15	$2^{-17.5}$
$(0,0,0,0,1,0,0,0,1,1,0,0,1,1,1,1) \xrightarrow{1r} (1,0,0,0,0,1,1,1,1,0,0,1,0,0,1,0)$	5,10,14,16,17,18	9,13,15,17,18	2^{-12}
$(0,0,0,0,1,0,0,0,1,1,0,1,0,0,0,0) \xrightarrow{1r} (0,1,1,0,1,1,1,1,0,0,0,0,1,1,0,0)$	5,10,12	9	2^{-12}
$(0,0,0,0,1,0,0,0,1,1,0,1,0,0,0,1) \xrightarrow{1r} (1,0,0,1,0,0,0,0,1,1,1,1,0,0,1,0)$	5,10,12,16,17,18	9,17,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,0,1,1,0,1,0,0,1,0) \xrightarrow{1r} (1,0,1,0,1,1,1,0,0,0,0,0,1,1,0,0)$	5,10,12,18	9,15,18	2^{-12}
$(0,0,0,0,1,0,0,0,1,1,0,1,0,0,1,1) \xrightarrow{1r} (0,1,0,1,0,0,0,1,1,1,1,1,0,0,1,0)$	5,10,12,16,17	9,15,17	$2^{-17.5}$
$(0,0,0,0,1,0,0,0,1,1,0,1,0,1,0,0) \xrightarrow{1r} (1,0,1,1,0,0,1,0,0,1,1,1,0,0,1,1)$	5,10,12,14,17,18	9,17,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,0,1,1,0,1,0,1,0,1) \xrightarrow{1r} (0,1,0,0,1,1,0,1,1,0,0,0,1,1,0,1)$	5,10,12,14,16	9	2^{-23}
$(0,0,0,0,1,0,0,0,1,1,0,1,0,1,1,0) \xrightarrow{1r} (0,1,1,1,0,0,1,1,0,1,1,1,0,0,1,1)$	5,10,12,14,17	9,15,17	$2^{-17.5}$
$(0,0,0,0,1,0,0,0,1,1,0,1,0,1,1,1) \xrightarrow{1r} (1,0,0,0,1,1,0,0,1,0,0,0,1,1,0,1)$	5,10,12,14,16,18	9,15,18	2^{-23}
$(0,0,0,0,1,0,0,0,1,1,0,1,1,0,0,0) \xrightarrow{1r} (1,0,1,1,1,0,1,1,0,1,0,0,1,1,0,0)$	5,10,12,18	9,13,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,0,1,1,0,1,1,0,0,1) \xrightarrow{1r} (0,1,0,0,0,1,0,0,1,0,1,1,0,0,1,0)$	5,10,12,16,17	9,13,17	2^{-23}
$(0,0,0,0,1,0,0,0,1,1,0,1,1,0,1,0) \xrightarrow{1r} (0,1,1,1,1,0,1,0,0,1,0,0,1,1,0,0)$	5,10,12	9,13,15	$2^{-17.5}$
$(0,0,0,0,1,0,0,0,1,1,0,1,1,0,1,1) \xrightarrow{1r} (1,0,0,0,0,1,0,1,1,0,1,1,0,0,1,0)$	5,10,12,16,17,18	9,13,15,17,18	2^{-23}
$(0,0,0,0,1,0,0,0,1,1,0,1,1,1,0,0) \xrightarrow{1r} (0,1,1,0,0,1,1,0,0,0,1,1,0,0,1,1)$	5,10,12,14,17	9,13,17	2^{-12}
$(0,0,0,0,1,0,0,0,1,1,0,1,1,1,0,1) \xrightarrow{1r} (1,0,0,1,1,0,0,1,1,1,0,0,1,1,0,1)$	5,10,12,14,16,18	9,13,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,0,1,1,0,1,1,1,1,0) \xrightarrow{1r} (1,0,1,0,0,1,1,1,0,0,1,1,0,0,1,1)$	5,10,12,14,17,18	9,13,15,17,18	2^{-12}
$(0,0,0,0,1,0,0,0,1,1,0,1,1,1,1,1) \xrightarrow{1r} (0,1,0,1,1,0,0,0,1,1,0,0,1,1,0,1)$	5,10,12,14,16	9,13,15	$2^{-17.5}$

Table 0.72 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	5,10,17	9,11,17	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	5,10,16,18	9,11,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	5,10,17,18	9,11,15,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	5,10,16	9,11,15	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	5,10,14,18	9,11,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	5,10,14,16,17	9,11,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	5,10,14	9,11,15	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	5,10,14,16,17,18	9,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	5,10,17,18	9,11,13,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	5,10,16	9,11,13	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	5,10,17	9,11,13,15,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	5,10,16,18	9,11,13,15,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	5,10,14	9,11,13	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	5,10,14,16,17,18	9,11,13,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	5,10,14,18	9,11,13,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	5,10,14,16,17	9,11,13,15,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	5,10,12,18	9,11,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	5,10,12,16,17	9,11,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	5,10,12	9,11,15	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	5,10,12,16,17,18	9,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	5,10,12,14,17	9,11,17	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	5,10,12,14,16,18	9,11,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	5,10,12,14,17,18	9,11,15,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	5,10,12,14,16	9,11,15	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	5,10,12	9,11,13	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	5,10,12,16,17,18	9,11,13,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	5,10,12,18	9,11,13,15,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	5,10,12,16,17	9,11,13,15,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	5,10,12,14,17,18	9,11,13,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	5,10,12,14,16	9,11,13	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	5,10,12,14,17	9,11,13,15,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	5,10,12,14,16,18	9,11,13,15,18	$2^{-17.5}$

Table 0.73 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,0,0,1,0,0,0,0,0,0,0,0) \xrightarrow{1r} (0,0,1,0,1,1,1,1,1,0,1,0,1,1,0,1)$	5,17	8,17	2^{-23}
$(0,0,0,0,1,0,0,1,0,0,0,0,0,0,0,1) \xrightarrow{1r} (1,1,0,1,0,0,0,0,0,1,0,1,0,0,1,1)$	5,16,18	8,18	$2^{-6.5}$
$(0,0,0,0,1,0,0,1,0,0,0,0,0,0,1,0) \xrightarrow{1r} (1,1,1,0,1,1,1,0,1,0,1,0,1,1,0,1)$	5,17,18	8,15,17,18	2^{-23}
$(0,0,0,0,1,0,0,1,0,0,0,0,0,0,1,1) \xrightarrow{1r} (0,0,0,1,0,0,0,1,0,1,0,1,0,0,1,1)$	5,16	8,15	$2^{-6.5}$
$(0,0,0,0,1,0,0,1,0,0,0,0,0,1,0,0) \xrightarrow{1r} (1,1,1,1,0,0,1,0,1,1,0,1,0,0,1,0)$	5,14,18	8,18	$2^{-6.5}$
$(0,0,0,0,1,0,0,1,0,0,0,0,0,1,0,1) \xrightarrow{1r} (0,0,0,0,1,1,0,1,0,0,1,0,1,1,0,0)$	5,14,16,17	8,17	2^{-12}
$(0,0,0,0,1,0,0,1,0,0,0,0,0,1,1,0) \xrightarrow{1r} (0,0,1,1,0,0,1,1,1,1,0,1,0,0,1,0)$	5,14	8,15	$2^{-6.5}$
$(0,0,0,0,1,0,0,1,0,0,0,0,0,1,1,1) \xrightarrow{1r} (1,1,0,0,1,1,0,0,0,0,1,0,1,1,0,0)$	5,14,16,17,18	8,15,17,18	2^{-12}
$(0,0,0,0,1,0,0,1,0,0,0,0,1,0,0,0) \xrightarrow{1r} (1,1,1,1,1,0,1,1,1,1,1,0,1,1,0,1)$	5,17,18	8,13,17,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,0,0,0,0,1,0,0,1) \xrightarrow{1r} (0,0,0,0,0,1,0,0,0,0,0,1,0,0,1,1)$	5,16	8,13	2^{-1}
$(0,0,0,0,1,0,0,1,0,0,0,0,1,0,1,0) \xrightarrow{1r} (0,0,1,1,1,0,1,0,1,1,1,0,1,1,0,1)$	5,17	8,13,15,17	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,0,0,0,0,1,0,1,1) \xrightarrow{1r} (1,1,0,0,0,1,0,1,0,0,0,1,0,0,1,1)$	5,16,18	8,13,15,18	2^{-1}
$(0,0,0,0,1,0,0,1,0,0,0,0,1,1,0,0) \xrightarrow{1r} (0,0,1,0,0,1,1,0,1,0,0,1,0,0,1,0)$	5,14	8,13	2^{-12}
$(0,0,0,0,1,0,0,1,0,0,0,0,1,1,0,1) \xrightarrow{1r} (1,1,0,1,1,0,0,1,0,1,1,0,1,1,0,0)$	5,14,16,17,18	8,13,17,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,0,0,0,0,1,1,1,0) \xrightarrow{1r} (1,1,1,0,0,1,1,1,1,0,0,1,0,0,1,0)$	5,14,18	8,13,15,18	2^{-12}
$(0,0,0,0,1,0,0,1,0,0,0,0,1,1,1,1) \xrightarrow{1r} (0,0,0,1,1,0,0,0,0,1,1,0,1,1,0,0)$	5,14,16,17	8,13,15,17	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,0,0,0,1,0,0,0,0) \xrightarrow{1r} (1,1,1,1,0,0,0,0,1,1,1,1,0,0,1,0)$	5,12,18	8,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,0,0,0,1,0,0,0,1) \xrightarrow{1r} (0,0,0,0,1,1,1,1,0,0,0,0,1,1,0,0)$	5,12,16,17	8,17	2^{-12}
$(0,0,0,0,1,0,0,1,0,0,0,1,0,0,1,0) \xrightarrow{1r} (0,0,1,1,0,0,0,1,1,1,1,1,0,0,1,0)$	5,12	8,15	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,0,0,0,1,0,0,1,1) \xrightarrow{1r} (1,1,0,0,1,1,1,0,0,0,0,0,1,1,0,0)$	5,12,16,17,18	8,15,17,18	2^{-12}
$(0,0,0,0,1,0,0,1,0,0,0,1,0,1,0,0) \xrightarrow{1r} (0,0,1,0,1,1,0,1,1,0,0,0,1,1,0,1)$	5,12,14,17	8,17	2^{-23}
$(0,0,0,0,1,0,0,1,0,0,0,1,0,1,0,1) \xrightarrow{1r} (1,1,0,1,0,0,1,0,0,1,1,1,0,0,1,1)$	5,12,14,16,18	8,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,0,0,0,1,0,1,1,0) \xrightarrow{1r} (1,1,1,0,1,1,0,0,1,0,0,0,1,1,0,1)$	5,12,14,17,18	8,15,17,18	2^{-23}
$(0,0,0,0,1,0,0,1,0,0,0,1,0,1,1,1) \xrightarrow{1r} (0,0,0,1,0,0,1,1,0,1,1,1,0,0,1,1)$	5,12,14,16	8,15	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,0,0,0,1,1,0,0,0) \xrightarrow{1r} (0,0,1,0,0,1,0,0,1,0,1,0,1,1,0,0,1,0)$	5,12	8,13	2^{-23}
$(0,0,0,0,1,0,0,1,0,0,0,1,1,0,0,1) \xrightarrow{1r} (1,1,0,1,1,0,1,1,0,1,0,1,0,0,1,1,0,0)$	5,12,16,17,18	8,13,17,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,0,0,0,1,1,0,1,0) \xrightarrow{1r} (1,1,1,0,0,1,0,1,1,0,1,1,0,0,1,0)$	5,12,18	8,13,15,18	2^{-23}
$(0,0,0,0,1,0,0,1,0,0,0,1,1,0,1,1) \xrightarrow{1r} (0,0,0,1,1,0,1,0,0,1,0,0,1,1,0,0)$	5,12,16,17	8,13,15,17	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,0,0,0,1,1,1,0,0) \xrightarrow{1r} (1,1,1,1,1,0,0,1,1,1,0,0,1,1,0,1)$	5,12,14,17,18	8,13,17,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,0,0,0,1,1,1,0,1) \xrightarrow{1r} (0,0,0,0,0,1,1,0,0,0,1,1,0,0,1,1)$	5,12,14,16	8,13	2^{-12}
$(0,0,0,0,1,0,0,1,0,0,0,1,1,1,1,0) \xrightarrow{1r} (0,0,1,1,1,0,0,0,1,1,0,0,1,1,0,1)$	5,12,14,17	8,13,15,17	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,0,0,0,1,1,1,1,1) \xrightarrow{1r} (1,1,0,0,0,1,1,1,0,0,1,1,0,0,1,1)$	5,12,14,16,18	8,13,15,18	2^{-12}

Table 0.74 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,0,0,1,0,0,1,0,0,0,0,0) \xrightarrow{1r} (1,1,1,0,1,0,1,1,1,1,1,1,1,1,0,1)$	5,17,18	8,11,17,18	2^{-23}
$(0,0,0,0,1,0,0,1,0,0,1,0,0,0,0,1) \xrightarrow{1r} (0,0,0,1,0,1,0,0,0,0,0,0,0,0,1,1)$	5,16	8,11	$2^{-6.5}$
$(0,0,0,0,1,0,0,1,0,0,1,0,0,0,1,0) \xrightarrow{1r} (0,0,1,0,1,0,1,0,1,1,1,1,1,1,0,1)$	5,17	8,11,15,17	2^{-23}
$(0,0,0,0,1,0,0,1,0,0,1,0,0,0,1,1) \xrightarrow{1r} (1,1,0,1,0,1,0,1,0,0,0,0,0,0,1,1)$	5,16,18	8,11,15,18	$2^{-6.5}$
$(0,0,0,0,1,0,0,1,0,0,1,0,0,1,0,0) \xrightarrow{1r} (0,0,1,1,0,1,1,0,1,0,0,0,0,0,1,0)$	5,14	8,11	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,0,0,1,0,0,1,0,1) \xrightarrow{1r} (1,1,0,0,1,0,0,1,0,1,1,1,1,1,0,0)$	5,14,16,17,18	8,11,17,18	2^{-23}
$(0,0,0,0,1,0,0,1,0,0,1,0,0,1,1,0) \xrightarrow{1r} (1,1,1,1,0,1,1,1,1,0,0,0,0,0,1,0)$	5,14,18	8,11,15,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,0,0,1,0,0,1,1,1) \xrightarrow{1r} (0,0,0,0,1,0,0,0,0,1,1,1,1,1,0,0)$	5,14,16,17	8,11,15,17	2^{-23}
$(0,0,0,0,1,0,0,1,0,0,1,0,1,0,0,0) \xrightarrow{1r} (0,0,1,1,1,1,1,1,0,1,1,1,1,0,1)$	5,17	8,11,13,17	$2^{-28.5}$
$(0,0,0,0,1,0,0,1,0,0,1,0,1,0,0,1) \xrightarrow{1r} (1,1,0,0,0,0,0,0,0,1,0,0,0,0,1,1)$	5,16,18	8,11,13,18	2^{-12}
$(0,0,0,0,1,0,0,1,0,0,1,0,1,0,1,0) \xrightarrow{1r} (1,1,1,1,1,1,1,0,1,0,1,1,1,1,0,1)$	5,17,18	8,11,13,15,17,18	$2^{-28.5}$
$(0,0,0,0,1,0,0,1,0,0,1,0,1,0,1,1) \xrightarrow{1r} (0,0,0,0,0,0,0,1,0,1,0,0,0,0,1,1)$	5,16	8,11,13,15	2^{-12}
$(0,0,0,0,1,0,0,1,0,0,1,0,1,1,0,0) \xrightarrow{1r} (1,1,1,0,0,0,1,0,1,1,0,0,0,0,1,0)$	5,14,18	8,11,13,18	2^{-12}
$(0,0,0,0,1,0,0,1,0,0,1,0,1,1,0,1) \xrightarrow{1r} (0,0,0,1,1,1,0,1,0,0,1,1,1,1,0,0)$	5,14,16,17	8,11,13,17	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,0,0,1,0,1,1,1,0) \xrightarrow{1r} (0,0,1,0,0,0,1,1,1,1,0,0,0,0,1,0)$	5,14	8,11,13,15	2^{-12}
$(0,0,0,0,1,0,0,1,0,0,1,0,1,1,1,1) \xrightarrow{1r} (1,1,0,1,1,1,0,0,0,0,1,1,1,1,0,0)$	5,14,16,17,18	8,11,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,0,0,1,1,0,0,0,0) \xrightarrow{1r} (0,0,1,1,0,1,0,0,1,0,1,0,0,0,1,0)$	5,12	8,11	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,0,0,1,1,0,0,0,1) \xrightarrow{1r} (1,1,0,0,1,0,1,1,0,1,0,1,1,1,0,0)$	5,12,16,17,18	8,11,17,18	2^{-12}
$(0,0,0,0,1,0,0,1,0,0,1,1,0,0,1,0) \xrightarrow{1r} (1,1,1,1,0,1,0,1,1,0,1,0,0,0,1,0)$	5,12,18	8,11,15,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,0,0,1,1,0,1,0,1) \xrightarrow{1r} (0,0,0,0,1,0,1,0,0,1,0,1,1,1,0,0)$	5,12,16,17	8,11,13,17	2^{-12}
$(0,0,0,0,1,0,0,1,0,0,1,1,0,1,1,0) \xrightarrow{1r} (0,0,1,0,0,0,1,1,1,1,0,0,0,0,1,0)$	5,14	8,11,13,15	2^{-12}
$(0,0,0,0,1,0,0,1,0,0,1,1,0,1,1,1) \xrightarrow{1r} (1,1,0,1,1,1,0,0,0,0,1,1,1,1,0,0)$	5,14,16,17,18	8,11,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,0,0,1,1,0,0,0,0) \xrightarrow{1r} (0,0,1,1,0,1,0,0,1,0,1,0,0,0,1,0)$	5,12	8,11	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,0,0,1,1,0,0,0,1) \xrightarrow{1r} (1,1,0,0,1,0,1,1,0,1,0,1,1,1,0,0)$	5,12,16,17,18	8,11,17,18	2^{-12}
$(0,0,0,0,1,0,0,1,0,0,1,1,0,0,1,0) \xrightarrow{1r} (1,1,1,1,0,1,0,1,1,0,1,0,0,0,1,0)$	5,12,18	8,11,15,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,0,0,1,1,0,0,1,1) \xrightarrow{1r} (0,0,0,0,1,0,1,0,0,1,0,1,1,1,0,0)$	5,12,16,17	8,11,15,17	2^{-12}
$(0,0,0,0,1,0,0,1,0,0,1,1,0,0,1,1) \xrightarrow{1r} (1,1,1,0,1,0,0,1,1,1,0,1,1,1,0,0)$	5,12,16,17,18	8,11,17,18	2^{-12}
$(0,0,0,0,1,0,0,1,0,0,1,1,0,1,0,1) \xrightarrow{1r} (0,0,0,1,0,1,1,0,0,0,1,0,0,0,1,1)$	5,12,14,16	8,11	$2^{-6.5}$
$(0,0,0,0,1,0,0,1,0,0,1,1,0,1,1,0) \xrightarrow{1r} (0,0,1,0,1,0,0,0,1,1,0,1,1,1,0,1)$	5,12,14,17	8,11,15,17	2^{-12}
$(0,0,0,0,1,0,0,1,0,0,1,1,0,1,1,1) \xrightarrow{1r} (1,1,0,1,0,1,1,1,0,0,1,0,0,0,1,1)$	5,12,14,16,18	8,11,15,18	$2^{-6.5}$
$(0,0,0,0,1,0,0,1,0,0,1,1,1,0,0,0) \xrightarrow{1r} (1,1,1,0,0,0,0,0,1,1,1,0,0,0,1,0)$	5,12,18	8,11,13,18	2^{-12}
$(0,0,0,0,1,0,0,1,0,0,1,1,1,0,0,1) \xrightarrow{1r} (0,0,0,1,1,1,1,1,0,0,0,1,1,1,0,0)$	5,12,16,17	8,11,13,17	$2^{-6.5}$
$(0,0,0,0,1,0,0,1,0,0,1,1,1,0,1,0) \xrightarrow{1r} (0,0,1,0,0,0,0,1,1,1,1,0,0,0,1,0)$	5,12	8,11,13,15	2^{-12}
$(0,0,0,0,1,0,0,1,0,0,1,1,1,0,1,1) \xrightarrow{1r} (1,1,0,1,1,1,1,0,0,0,0,1,1,1,0,0)$	5,12,16,17,18	8,11,13,15,17,18	$2^{-6.5}$
$(0,0,0,0,1,0,0,1,0,0,1,1,1,1,0,0) \xrightarrow{1r} (0,0,1,1,1,1,0,1,1,0,0,1,1,1,0,1)$	5,12,14,17	8,11,13,17	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,0,0,1,1,1,1,0,1) \xrightarrow{1r} (1,1,0,0,0,0,1,0,0,1,1,0,0,0,1,1)$	5,12,14,16,18	8,11,13,18	2^{-12}
$(0,0,0,0,1,0,0,1,0,0,1,1,1,1,1,0) \xrightarrow{1r} (1,1,1,1,1,1,0,0,1,0,0,1,1,1,0,1)$	5,12,14,17,18	8,11,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,0,0,1,1,1,1,1,1) \xrightarrow{1r} (0,0,0,0,0,0,1,1,0,1,1,0,0,0,1,1)$	5,12,14,16	8,11,13,15	2^{-12}

Table 0.75 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	5,10,18	8,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	5,10,16,17	8,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	5,10	8,15	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	5,10,16,17,18	8,15,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	5,10,14,17	8,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	5,10,14,16,18	8,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	5,10,14,17,18	8,15,17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	5,10,14,16	8,15	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	5,10	8,13	2^{-34}
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	5,10,16,17,18	8,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	5,10,18	8,13,15,18	2^{-34}
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	5,10,16,17	8,13,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	5,10,14,17,18	8,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	5,10,14,16	8,13	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	5,10,14,17	8,13,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	5,10,14,16,18	8,13,15,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	5,10,12,17	8,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	5,10,12,16,18	8,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	5,10,12,17,18	8,15,17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	5,10,12,16	8,15	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	5,10,12,14,18	8,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	5,10,12,14,16,17	8,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	5,10,12,14	8,15	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	5,10,12,14,16,17,18	8,15,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	5,10,12,17,18	8,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	5,10,12,16	8,13	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	5,10,12,17	8,13,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	5,10,12,16,18	8,13,15,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	5,10,12,14	8,13	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	5,10,12,14,16,17,18	8,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	5,10,12,14,18	8,13,15,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	5,10,12,14,16,17	8,13,15,17	$2^{-17.5}$

Table 0.76 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	5,10	8,11	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	5,10,16,17,18	8,11,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	5,10,18	8,11,15,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	5,10,16,17	8,11,15,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	5,10,14,17,18	8,11,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	5,10,14,16	8,11	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	5,10,14,17	8,11,15,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	5,10,14,16,18	8,11,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	5,10,18	8,11,13,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	5,10,16,17	8,11,13,17	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	5,10	8,11,13,15	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	5,10,16,17,18	8,11,13,15,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	5,10,14,17	8,11,13,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	5,10,14,16,18	8,11,13,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	5,10,14,17,18	8,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	5,10,14,16	8,11,13,15	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	5,10,12,17,18	8,11,17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	5,10,12,16	8,11	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	5,10,12,17	8,11,15,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	5,10,12,16,18	8,11,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	5,10,12,14	8,11	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	5,10,12,14,16,17,18	8,11,17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	5,10,12,14,18	8,11,15,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	5,10,12,14,16,17	8,11,15,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	5,10,12,17	8,11,13,17	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	5,10,12,16,18	8,11,13,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	5,10,12,17,18	8,11,13,15,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	5,10,12,16	8,11,13,15	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	5,10,12,14,18	8,11,13,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	5,10,12,14,16,17	8,11,13,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	5,10,12,14	8,11,13,15	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	5,10,12,14,16,17,18	8,11,13,15,17,18	$2^{-17.5}$

Table 0.77 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,0,0,1,1,0,0,0,0,0,0,0) \xrightarrow{1r} (1,0,1,1,1,0,1,0,1,1,1,1,1,1,0,0,1)$	5,17,18	8,9,17,18	$2^{-28.5}$
$(0,0,0,0,1,0,0,1,1,0,0,0,0,0,0,1) \xrightarrow{1r} (0,1,0,0,0,1,0,1,0,0,0,0,0,0,1,1,1)$	5,16	8,9	2^{-12}
$(0,0,0,0,1,0,0,1,1,0,0,0,0,0,1,0) \xrightarrow{1r} (0,1,1,1,1,0,1,1,1,1,1,1,1,1,0,0,1)$	5,17	8,9,15,17	$2^{-28.5}$
$(0,0,0,0,1,0,0,1,1,0,0,0,0,0,1,1) \xrightarrow{1r} (1,0,0,0,0,1,0,0,0,0,0,0,0,0,1,1,1)$	5,16,18	8,9,15,18	2^{-12}
$(0,0,0,0,1,0,0,1,1,0,0,0,0,1,0,0) \xrightarrow{1r} (0,1,1,0,0,1,1,1,1,0,0,0,0,1,1,0)$	5,14	8,9	2^{-23}
$(0,0,0,0,1,0,0,1,1,0,0,0,0,1,0,1) \xrightarrow{1r} (1,0,0,1,1,0,0,0,0,1,1,1,1,1,0,0,0)$	5,14,16,17,18	8,9,17,18	$2^{-28.5}$
$(0,0,0,0,1,0,0,1,1,0,0,0,0,1,1,0) \xrightarrow{1r} (1,0,1,0,0,1,1,0,1,0,0,0,0,0,1,1,0)$	5,14,18	8,9,15,18	2^{-23}
$(0,0,0,0,1,0,0,1,1,0,0,0,0,1,1,1) \xrightarrow{1r} (0,1,0,1,1,0,0,1,0,1,1,1,1,1,0,0,0)$	5,14,16,17	8,9,15,17	$2^{-28.5}$
$(0,0,0,0,1,0,0,1,1,0,0,0,1,0,0,0) \xrightarrow{1r} (0,1,1,0,1,1,1,0,1,0,1,1,1,1,0,0,1)$	5,17	8,9,13,17	2^{-34}
$(0,0,0,0,1,0,0,1,1,0,0,0,1,0,0,1) \xrightarrow{1r} (1,0,0,1,0,0,0,1,0,1,0,0,0,0,1,1,1)$	5,16,18	8,9,13,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,1,0,0,0,1,0,1,0) \xrightarrow{1r} (1,0,1,0,1,1,1,1,1,0,1,1,1,0,0,0,1)$	5,17,18	8,9,13,15,17,18	2^{-34}
$(0,0,0,0,1,0,0,1,1,0,0,0,1,0,1,1) \xrightarrow{1r} (0,1,0,1,0,0,0,0,0,1,0,0,0,0,1,1,1)$	5,16	8,9,13,15	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,1,0,0,0,1,1,0,0) \xrightarrow{1r} (1,0,1,1,0,0,1,1,1,1,0,0,0,0,1,1,0)$	5,14,18	8,9,13,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,1,0,0,0,1,1,0,1) \xrightarrow{1r} (0,1,0,0,1,1,0,0,0,0,1,1,1,0,0,0,0)$	5,14,16,17	8,9,13,17	2^{-23}
$(0,0,0,0,1,0,0,1,1,0,0,0,1,1,1,0) \xrightarrow{1r} (0,1,1,1,0,0,1,0,1,1,0,0,0,0,1,1,0)$	5,14	8,9,13,15	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,1,0,0,0,1,1,1,1) \xrightarrow{1r} (1,0,0,0,1,1,0,1,0,0,1,1,1,0,0,0,0)$	5,14,16,17,18	8,9,13,15,17,18	2^{-23}
$(0,0,0,0,1,0,0,1,1,0,0,1,0,0,0,0) \xrightarrow{1r} (0,1,1,0,0,1,0,1,1,0,1,0,0,0,1,1,0)$	5,12	8,9	2^{-23}
$(0,0,0,0,1,0,0,1,1,0,0,1,0,0,0,1) \xrightarrow{1r} (1,0,0,1,1,0,1,0,0,1,0,1,1,0,0,0,0)$	5,12,16,17,18	8,9,17,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,1,0,0,1,0,0,1,0) \xrightarrow{1r} (1,0,1,0,0,1,0,0,1,0,1,0,0,0,1,1,0)$	5,12,18	8,9,15,18	2^{-23}
$(0,0,0,0,1,0,0,1,1,0,0,1,0,0,1,1) \xrightarrow{1r} (0,1,0,1,1,0,1,1,0,1,0,1,1,0,0,0,0)$	5,12,16,17	8,9,15,17	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,1,0,0,1,0,1,0,0) \xrightarrow{1r} (1,0,1,1,1,0,0,0,1,1,0,1,1,1,0,0,1)$	5,12,14,17,18	8,9,17,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,1,0,0,1,0,1,0,1) \xrightarrow{1r} (0,1,0,0,0,1,1,1,0,0,1,0,0,0,1,1,1)$	5,12,14,16	8,9	2^{-12}
$(0,0,0,0,1,0,0,1,1,0,0,1,0,1,1,0) \xrightarrow{1r} (0,1,1,1,1,0,0,1,1,1,0,1,1,0,0,1)$	5,12,14,17	8,9,15,17	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,1,0,0,1,0,1,1,1) \xrightarrow{1r} (1,0,0,0,0,1,1,0,0,0,1,0,0,0,1,1,1)$	5,12,14,16,18	8,9,15,18	2^{-12}
$(0,0,0,0,1,0,0,1,1,0,0,1,1,0,0,0) \xrightarrow{1r} (1,0,1,1,0,0,0,1,1,1,1,0,0,0,1,1,0)$	5,12,18	8,9,13,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,1,0,0,1,1,0,0,1) \xrightarrow{1r} (0,1,0,0,1,1,1,0,0,0,0,1,1,0,0,0,0)$	5,12,16,17	8,9,13,17	2^{-12}
$(0,0,0,0,1,0,0,1,1,0,0,1,1,0,1,0) \xrightarrow{1r} (0,1,1,1,0,0,0,0,1,1,1,0,0,0,1,1,0)$	5,12	8,9,13,15	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,1,0,0,1,1,0,1,1) \xrightarrow{1r} (1,0,0,0,1,1,1,1,0,0,0,1,1,0,0,0,0)$	5,12,16,17,18	8,9,13,15,17,18	2^{-12}
$(0,0,0,0,1,0,0,1,1,0,0,1,1,1,0,0) \xrightarrow{1r} (0,1,1,0,1,1,0,0,1,0,0,1,1,0,0,1)$	5,12,14,17	8,9,13,17	2^{-23}
$(0,0,0,0,1,0,0,1,1,0,0,1,1,1,0,1) \xrightarrow{1r} (1,0,0,1,0,0,1,1,0,1,1,0,0,0,1,1,1)$	5,12,14,16,18	8,9,13,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,1,0,0,1,1,1,1,0) \xrightarrow{1r} (1,0,1,0,1,1,0,1,1,0,0,1,1,0,0,1,1)$	5,12,14,17,18	8,9,13,15,17,18	2^{-23}
$(0,0,0,0,1,0,0,1,1,0,0,1,1,1,1,1) \xrightarrow{1r} (0,1,0,1,0,0,1,0,0,1,1,0,0,1,1,1)$	5,12,14,16	8,9,13,15	$2^{-17.5}$

Table 0.78 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,0,0,1,1,0,1,0,0,0,0,0) \xrightarrow{1r} (0,1,1,1,1,1,1,0,1,0,1,0,1,0,0,1)$	5,17	8,9,11,17	$2^{-28.5}$
$(0,0,0,0,1,0,0,1,1,0,1,0,0,0,0,1) \xrightarrow{1r} (1,0,0,0,0,0,0,1,0,1,0,1,0,1,1,1)$	5,16,18	8,9,11,18	2^{-12}
$(0,0,0,0,1,0,0,1,1,0,1,0,0,0,1,0) \xrightarrow{1r} (1,0,1,1,1,1,1,1,0,1,0,1,0,0,1)$	5,17,18	8,9,11,15,17,18	$2^{-28.5}$
$(0,0,0,0,1,0,0,1,1,0,1,0,0,0,1,1) \xrightarrow{1r} (0,1,0,0,0,0,0,0,0,1,0,1,0,1,1,1)$	5,16	8,9,11,15	2^{-12}
$(0,0,0,0,1,0,0,1,1,0,1,0,0,1,0,0) \xrightarrow{1r} (1,0,1,0,0,0,1,1,1,1,0,1,0,1,1,0)$	5,14,18	8,9,11,18	2^{-12}
$(0,0,0,0,1,0,0,1,1,0,1,0,0,1,0,1) \xrightarrow{1r} (0,1,0,1,1,1,0,0,0,0,1,0,1,0,0,0)$	5,14,16,17	8,9,11,17	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,1,0,1,0,0,1,1,0) \xrightarrow{1r} (0,1,1,0,0,0,1,0,1,1,0,1,0,1,1,0)$	5,14	8,9,11,15	2^{-12}
$(0,0,0,0,1,0,0,1,1,0,1,0,0,1,1,1) \xrightarrow{1r} (1,0,0,1,1,1,0,1,0,0,1,0,1,0,0,0)$	5,14,16,17,18	8,9,11,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,1,0,1,0,1,0,0,0) \xrightarrow{1r} (1,0,1,0,1,0,1,0,1,1,1,1,0,1,0,0,1)$	5,17,18	8,9,11,13,17,18	2^{-23}
$(0,0,0,0,1,0,0,1,1,0,1,0,1,0,0,1) \xrightarrow{1r} (0,1,0,1,0,1,0,1,0,0,0,1,0,1,1,1)$	5,16	8,9,11,13	$2^{-6.5}$
$(0,0,0,0,1,0,0,1,1,0,1,0,1,0,1,0) \xrightarrow{1r} (0,1,1,0,1,0,1,1,1,1,1,0,1,0,0,1)$	5,17	8,9,11,13,15,17	2^{-23}
$(0,0,0,0,1,0,0,1,1,0,1,0,1,0,1,1) \xrightarrow{1r} (1,0,0,1,0,1,0,0,0,0,1,0,1,1,1,1)$	5,16,18	8,9,11,13,15,18	$2^{-6.5}$
$(0,0,0,0,1,0,0,1,1,0,1,0,1,1,0,0) \xrightarrow{1r} (0,1,1,1,0,1,1,1,1,0,0,1,0,1,1,0)$	5,14	8,9,11,13	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,1,0,1,0,1,1,0,1) \xrightarrow{1r} (1,0,0,0,1,0,0,0,0,1,1,0,1,0,0,0)$	5,14,16,17,18	8,9,11,13,17,18	2^{-23}
$(0,0,0,0,1,0,0,1,1,0,1,0,1,1,1,0) \xrightarrow{1r} (1,0,1,1,0,1,1,0,1,0,0,1,0,1,1,0)$	5,14,18	8,9,11,13,15,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,1,0,1,0,1,1,1,1) \xrightarrow{1r} (0,1,0,0,1,0,0,1,0,1,1,0,1,0,0,0)$	5,14,16,17	8,9,11,13,15,17	2^{-23}
$(0,0,0,0,1,0,0,1,1,0,1,1,0,0,0,0) \xrightarrow{1r} (1,0,1,0,0,0,0,1,1,1,1,1,0,1,1,0)$	5,12,18	8,9,11,18	2^{-23}
$(0,0,0,0,1,0,0,1,1,0,1,1,0,0,0,1) \xrightarrow{1r} (0,1,0,1,1,1,1,0,0,0,0,1,0,0,0,0)$	5,12,16,17	8,9,11,17	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,1,0,1,1,0,0,1,0) \xrightarrow{1r} (0,1,1,0,0,0,0,0,1,1,1,1,0,1,1,0)$	5,12	8,9,11,15	2^{-23}
$(0,0,0,0,1,0,0,1,1,0,1,1,0,0,1,1) \xrightarrow{1r} (1,0,0,1,1,1,1,1,0,0,0,0,1,0,0,0)$	5,12,16,17,18	8,9,11,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,1,0,1,1,0,1,0,0) \xrightarrow{1r} (0,1,1,1,1,1,0,0,1,0,0,0,1,0,0,1)$	5,12,14,17	8,9,11,17	$2^{-28.5}$
$(0,0,0,0,1,0,0,1,1,0,1,1,0,1,0,1) \xrightarrow{1r} (1,0,0,0,0,0,1,1,0,1,1,1,0,1,1,1)$	5,12,14,16,18	8,9,11,18	2^{-23}
$(0,0,0,0,1,0,0,1,1,0,1,1,0,1,1,0) \xrightarrow{1r} (1,0,1,1,1,1,0,1,1,0,0,0,1,0,0,1)$	5,12,14,17,18	8,9,11,15,17,18	$2^{-28.5}$
$(0,0,0,0,1,0,0,1,1,0,1,1,0,1,1,1) \xrightarrow{1r} (0,1,0,0,0,0,1,0,0,1,1,1,0,1,1,1)$	5,12,14,16	8,9,11,15	2^{-23}
$(0,0,0,0,1,0,0,1,1,0,1,1,1,0,0,0) \xrightarrow{1r} (0,1,1,1,0,1,0,1,1,0,1,1,0,1,1,0)$	5,12	8,9,11,13	$2^{-28.5}$
$(0,0,0,0,1,0,0,1,1,0,1,1,1,0,0,1) \xrightarrow{1r} (1,0,0,0,1,0,1,0,0,1,0,0,1,0,0,0)$	5,12,16,17,18	8,9,11,13,17,18	2^{-23}
$(0,0,0,0,1,0,0,1,1,0,1,1,1,0,1,0) \xrightarrow{1r} (1,0,1,1,0,1,0,0,1,0,1,1,0,1,1,0)$	5,12,18	8,9,11,13,15,18	$2^{-28.5}$
$(0,0,0,0,1,0,0,1,1,0,1,1,1,0,1,1) \xrightarrow{1r} (0,1,0,0,1,0,1,1,0,1,0,0,1,0,0,0)$	5,12,16,17	8,9,11,13,15,17	2^{-23}
$(0,0,0,0,1,0,0,1,1,0,1,1,1,1,0,0) \xrightarrow{1r} (1,0,1,0,1,0,0,0,1,1,0,0,1,0,0,1)$	5,12,14,17,18	8,9,11,13,17,18	2^{-23}
$(0,0,0,0,1,0,0,1,1,0,1,1,1,1,0,1) \xrightarrow{1r} (0,1,0,1,0,1,1,1,0,0,1,1,0,1,1,1)$	5,12,14,16	8,9,11,13	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,1,0,1,1,1,1,1,0) \xrightarrow{1r} (0,1,1,0,1,0,0,1,1,1,0,0,1,0,0,1)$	5,12,14,17	8,9,11,13,15,17	2^{-23}
$(0,0,0,0,1,0,0,1,1,0,1,1,1,1,1,1) \xrightarrow{1r} (1,0,0,1,0,1,1,0,0,0,1,1,0,1,1,1)$	5,12,14,16,18	8,9,11,13,15,18	$2^{-17.5}$

Table 0.79 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,0,0,1,1,1,0,0,0,0,0,0) \xrightarrow{1r} (0,1,0,0,1,1,1,1,1,0,1,0,1,1,1,0)$	5,10	8,9	2^{-23}
$(0,0,0,0,1,0,0,1,1,1,0,0,0,0,0,1) \xrightarrow{1r} (1,0,1,1,0,0,0,0,0,1,0,1,0,0,0,0)$	5,10,16,17,18	8,9,17,18	$2^{-6.5}$
$(0,0,0,0,1,0,0,1,1,1,0,0,0,0,1,0) \xrightarrow{1r} (1,0,0,0,1,1,1,0,1,0,1,0,1,1,1,0)$	5,10,18	8,9,15,18	2^{-23}
$(0,0,0,0,1,0,0,1,1,1,0,0,0,0,1,1) \xrightarrow{1r} (0,1,1,1,0,0,0,1,0,1,0,1,0,0,0,0)$	5,10,16,17	8,9,15,17	$2^{-6.5}$
$(0,0,0,0,1,0,0,1,1,1,0,0,0,1,0,0) \xrightarrow{1r} (1,0,0,1,0,0,1,0,1,1,0,1,0,0,0,1)$	5,10,14,17,18	8,9,17,18	$2^{-6.5}$
$(0,0,0,0,1,0,0,1,1,1,0,0,0,1,0,1) \xrightarrow{1r} (0,1,1,0,1,1,0,1,0,0,1,0,1,1,1,1)$	5,10,14,16	8,9	2^{-12}
$(0,0,0,0,1,0,0,1,1,1,0,0,0,1,1,0) \xrightarrow{1r} (0,1,0,1,0,0,1,1,1,1,0,1,0,0,0,1)$	5,10,14,17	8,9,15,17	$2^{-6.5}$
$(0,0,0,0,1,0,0,1,1,1,0,0,0,1,1,1) \xrightarrow{1r} (1,0,1,0,1,1,0,0,0,0,1,0,1,1,1,1)$	5,10,14,16,18	8,9,15,18	2^{-12}
$(0,0,0,0,1,0,0,1,1,1,0,0,1,0,0,0) \xrightarrow{1r} (1,0,0,1,1,0,1,1,1,1,1,0,1,1,1,0)$	5,10,18	8,9,13,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,1,1,0,0,1,0,0,1) \xrightarrow{1r} (0,1,1,0,0,1,0,0,0,0,0,1,0,0,0,0)$	5,10,16,17	8,9,13,17	2^{-1}
$(0,0,0,0,1,0,0,1,1,1,0,0,1,0,1,0) \xrightarrow{1r} (0,1,0,1,1,0,1,0,1,1,1,0,1,1,1,0)$	5,10	8,9,13,15	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,1,1,0,0,1,0,1,1) \xrightarrow{1r} (1,0,1,0,0,1,0,1,0,0,0,1,0,0,0,0)$	5,10,16,17,18	8,9,13,15,17,18	2^{-1}
$(0,0,0,0,1,0,0,1,1,1,0,0,1,1,0,0) \xrightarrow{1r} (0,1,0,0,0,1,1,0,1,0,0,1,0,0,0,1)$	5,10,14,17	8,9,13,17	2^{-12}
$(0,0,0,0,1,0,0,1,1,1,0,0,1,1,0,1) \xrightarrow{1r} (1,0,1,1,1,0,0,1,0,1,1,0,1,1,1,1)$	5,10,14,16,18	8,9,13,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,1,1,0,0,1,1,1,0) \xrightarrow{1r} (1,0,0,0,0,1,1,1,1,0,0,1,0,0,0,1)$	5,10,14,17,18	8,9,13,15,17,18	2^{-12}
$(0,0,0,0,1,0,0,1,1,1,0,0,1,1,1,1) \xrightarrow{1r} (0,1,1,1,1,0,0,0,0,1,1,0,1,1,1,1)$	5,10,14,16	8,9,13,15	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,1,1,0,1,0,0,0,0) \xrightarrow{1r} (1,0,0,1,0,0,0,0,0,1,1,1,1,0,0,0,1)$	5,10,12,17,18	8,9,17,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,1,1,0,1,0,0,0,1) \xrightarrow{1r} (0,1,1,0,1,1,1,1,0,0,0,0,1,1,1,1)$	5,10,12,16	8,9	2^{-12}
$(0,0,0,0,1,0,0,1,1,1,0,1,0,0,1,0) \xrightarrow{1r} (0,1,0,1,0,0,0,1,1,1,1,1,0,0,0,1)$	5,10,12,17	8,9,15,17	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,1,1,0,1,0,0,1,1) \xrightarrow{1r} (1,0,1,0,1,1,1,0,0,0,0,0,1,1,1,1)$	5,10,12,16,18	8,9,15,18	2^{-12}
$(0,0,0,0,1,0,0,1,1,1,0,1,0,1,0,0) \xrightarrow{1r} (0,1,0,0,1,1,0,1,1,0,0,0,1,1,1,0)$	5,10,12,14	8,9	2^{-23}
$(0,0,0,0,1,0,0,1,1,1,0,1,0,1,0,1) \xrightarrow{1r} (1,0,1,1,0,0,1,0,0,1,1,1,0,0,0,0)$	5,10,12,14,16,17,18	8,9,17,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,1,1,0,1,0,1,1,0) \xrightarrow{1r} (1,0,0,0,1,1,0,0,1,0,0,0,1,1,1,0)$	5,10,12,14,18	8,9,15,18	2^{-23}
$(0,0,0,0,1,0,0,1,1,1,0,1,0,1,1,1) \xrightarrow{1r} (0,1,1,1,0,0,1,1,0,1,1,1,0,0,0,0)$	5,10,12,14,16,17	8,9,15,17	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,1,1,0,1,1,0,0,0) \xrightarrow{1r} (0,1,0,0,0,1,0,0,1,0,1,1,0,0,0,1)$	5,10,12,17	8,9,13,17	2^{-23}
$(0,0,0,0,1,0,0,1,1,1,0,1,1,0,0,1) \xrightarrow{1r} (1,0,1,1,1,0,1,1,0,1,0,1,0,0,1,1,1,1)$	5,10,12,16,18	8,9,13,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,1,1,0,1,1,0,1,0) \xrightarrow{1r} (1,0,0,0,0,1,0,1,1,0,1,1,0,0,0,1)$	5,10,12,17,18	8,9,13,15,17,18	2^{-23}
$(0,0,0,0,1,0,0,1,1,1,0,1,1,0,1,1) \xrightarrow{1r} (0,1,1,1,1,0,1,0,0,1,0,0,1,1,1,1)$	5,10,12,16	8,9,13,15	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,1,1,0,1,1,1,0,0) \xrightarrow{1r} (1,0,0,1,1,0,0,1,1,1,0,0,1,1,1,0)$	5,10,12,14,18	8,9,13,18	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,1,1,0,1,1,1,0,1) \xrightarrow{1r} (0,1,1,0,0,1,1,0,0,0,1,1,0,0,0,0)$	5,10,12,14,16,17	8,9,13,17	2^{-12}
$(0,0,0,0,1,0,0,1,1,1,0,1,1,1,1,0) \xrightarrow{1r} (0,1,0,1,1,0,0,0,1,1,0,0,1,1,1,0)$	5,10,12,14	8,9,13,15	$2^{-17.5}$
$(0,0,0,0,1,0,0,1,1,1,0,1,1,1,1,1) \xrightarrow{1r} (1,0,1,0,0,1,1,1,0,0,1,1,0,0,0,0)$	5,10,12,14,16,17,18	8,9,13,15,17,18	2^{-12}

Table 0.80 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	5,10,18	8,9,11,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	5,10,16,17	8,9,11,17	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	5,10	8,9,11,15	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	5,10,16,17,18	8,9,11,15,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	5,10,14,17	8,9,11,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	5,10,14,16,18	8,9,11,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	5,10,14,17,18	8,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	5,10,14,16	8,9,11,15	2^{-23}
$(0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	5,10	8,9,11,13	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	5,10,16,17,18	8,9,11,13,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	5,10,18	8,9,11,13,15,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	5,10,16,17	8,9,11,13,15,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	5,10,14,17,18	8,9,11,13,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	5,10,14,16	8,9,11,13	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	5,10,14,17	8,9,11,13,15,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	5,10,14,16,18	8,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	5,10,12,17	8,9,11,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	5,10,12,16,18	8,9,11,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	5,10,12,17,18	8,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	5,10,12,16	8,9,11,15	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	5,10,12,14,18	8,9,11,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	5,10,12,17,18	8,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	5,10,12,14,16,17	8,9,11,17	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	5,10,12,14	8,9,11,15	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	5,10,12,14,16,17,18	8,9,11,15,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	5,10,12,17,18	8,9,11,13,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	5,10,12,16	8,9,11,13	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	5,10,12,17	8,9,11,13,15,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	5,10,12,16,18	8,9,11,13,15,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	5,10,12,14	8,9,11,13	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	5,10,12,14,16,17,18	8,9,11,13,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	5,10,12,14,18	8,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	5,10,12,14,16,17	8,9,11,13,15,17	2^{-12}

Table 0.81 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	5,7	—	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	5,7,16,17,18	17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	5,7,18	15,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	5,7,16,17	15,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	5,7,14,17,18	17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	5,7,14,16	—	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	5,7,14,17	15,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	5,7,14,16,18	15,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	5,7,18	13,18	2^{-1}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	5,7,16,17	13,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	5,7	13,15	2^{-1}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	5,7,16,17,18	13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	5,7,14,17	13,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	5,7,14,16,18	13,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	5,7,14,17,18	13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	5,7,14,16	13,15	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	5,7,12,17,18	17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	5,7,12,16	—	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	5,7,12,17	15,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	5,7,12,16,18	15,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	5,7,12,14	—	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	5,7,12,14,16,17,18	17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	5,7,12,14,18	15,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	5,7,12,14,16,17	15,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	5,7,12,17	13,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	5,7,12,16,18	13,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	5,7,12,17,18	13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	5,7,12,16	13,15	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	5,7,12,14,18	13,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	5,7,12,14,16,17	13,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	5,7,12,14	13,15	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	5,7,12,14,16,17,18	13,15,17,18	$2^{-17.5}$

Table 0.82 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	5,7,18	11,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	5,7,16,17	11,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	5,7	11,15	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	5,7,16,17,18	11,15,17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	5,7,14,17	11,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	5,7,14,16,18	11,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	5,7,14,17,18	11,15,17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	5,7,14,16	11,15	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	5,7	11,13	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	5,7,16,17,18	11,13,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	5,7,18	11,13,15,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	5,7,16,17	11,13,15,17	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	5,7,14,17,18	11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	5,7,14,16	11,13	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	5,7,14,17	11,13,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	5,7,14,16,18	11,13,15,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	5,7,12,17	11,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	5,7,12,16,18	11,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	5,7,12,17,18	11,15,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	5,7,12,16	11,15	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	5,7,12,14,18	11,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	5,7,12,14,16,17	11,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	5,7,12,14	11,15	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	5,7,12,14,16,17,18	11,15,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	5,7,12,17,18	11,13,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	5,7,12,16	11,13	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	5,7,12,17	11,13,15,17	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	5,7,12,16,18	11,13,15,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	5,7,12,14	11,13	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	5,7,12,14,16,17,18	11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	5,7,12,14,18	11,13,15,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	5,7,12,14,16,17	11,13,15,17	$2^{-17.5}$

Table 0.83 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,0,1,0,0,1,0,0,0,0,0,0) \xrightarrow{1r} (1,1,1,0,0,1,0,1,0,0,0,0,0,0,1,1)$	5,7,10,17,18	17,18	2^{-12}
$(0,0,0,0,1,0,1,0,0,1,0,0,0,0,0,1) \xrightarrow{1r} (0,0,0,1,1,0,1,0,1,1,1,1,1,1,0,1)$	5,7,10,16	—	$2^{-28.5}$
$(0,0,0,0,1,0,1,0,0,1,0,0,0,0,1,0) \xrightarrow{1r} (0,0,1,0,0,1,0,0,0,0,0,0,0,0,1,1)$	5,7,10,17	15,17	2^{-12}
$(0,0,0,0,1,0,1,0,0,1,0,0,0,0,1,1) \xrightarrow{1r} (1,1,0,1,1,0,1,1,1,1,1,1,1,1,0,1)$	5,7,10,16,18	15,18	$2^{-28.5}$
$(0,0,0,0,1,0,1,0,0,1,0,0,0,1,0,0) \xrightarrow{1r} (0,0,1,1,1,0,0,0,0,1,1,1,1,1,0,0)$	5,7,10,14	—	$2^{-28.5}$
$(0,0,0,0,1,0,1,0,0,1,0,0,0,1,0,1) \xrightarrow{1r} (1,1,0,0,0,1,1,1,1,0,0,0,0,0,1,0)$	5,7,10,14,16,17,18	17,18	2^{-23}
$(0,0,0,0,1,0,1,0,0,1,0,0,0,1,1,0) \xrightarrow{1r} (1,1,1,1,1,0,0,1,0,1,1,1,1,1,0,0)$	5,7,10,14,18	15,18	$2^{-28.5}$
$(0,0,0,0,1,0,1,0,0,1,0,0,0,1,1,1) \xrightarrow{1r} (0,0,0,0,0,1,1,0,1,0,0,0,0,0,1,0)$	5,7,10,14,16,17	15,17	2^{-23}
$(0,0,0,0,1,0,1,0,0,1,0,0,1,0,0,0) \xrightarrow{1r} (0,0,1,1,0,0,0,1,0,1,0,1,0,0,0,1,1)$	5,7,10,17	13,17	$2^{-17.5}$
$(0,0,0,0,1,0,1,0,0,1,0,0,1,0,0,1) \xrightarrow{1r} (1,1,0,0,1,1,1,0,1,0,1,1,1,1,0,1)$	5,7,10,16,18	13,18	2^{-34}
$(0,0,0,0,1,0,1,0,0,1,0,0,1,0,1,0) \xrightarrow{1r} (1,1,1,1,0,0,0,0,0,1,0,0,0,0,1,1)$	5,7,10,17,18	13,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,0,1,0,0,1,0,0,1,0,1,1) \xrightarrow{1r} (0,0,0,0,1,1,1,1,1,0,1,1,1,1,0,1)$	5,7,10,16	13,15	2^{-34}
$(0,0,0,0,1,0,1,0,0,1,0,0,1,1,0,0) \xrightarrow{1r} (1,1,1,0,1,1,0,0,0,0,1,1,1,1,0,0)$	5,7,10,14,18	13,18	2^{-23}
$(0,0,0,0,1,0,1,0,0,1,0,0,1,1,0,1) \xrightarrow{1r} (0,0,0,1,0,0,1,1,1,1,0,0,0,0,1,0)$	5,7,10,14,16,17	13,17	$2^{-17.5}$
$(0,0,0,0,1,0,1,0,0,1,0,0,1,1,1,0) \xrightarrow{1r} (0,0,1,0,1,1,0,1,0,0,1,1,1,1,0,0)$	5,7,10,14	13,15	2^{-23}
$(0,0,0,0,1,0,1,0,0,1,0,0,1,1,1,1) \xrightarrow{1r} (1,1,0,1,0,0,1,0,1,1,0,0,0,0,1,0)$	5,7,10,14,16,17,18	13,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,0,1,0,0,1,0,1,0,0,0,0) \xrightarrow{1r} (0,0,1,1,1,0,1,0,0,1,0,1,1,1,0,0)$	5,7,10,12	—	$2^{-17.5}$
$(0,0,0,0,1,0,1,0,0,1,0,1,0,0,0,1) \xrightarrow{1r} (1,1,0,0,0,1,0,1,1,0,1,0,0,0,1,0)$	5,7,10,12,16,17,18	17,18	2^{-23}
$(0,0,0,0,1,0,1,0,0,1,0,1,0,0,1,0) \xrightarrow{1r} (1,1,1,1,1,0,1,1,0,1,0,1,1,1,0,0)$	5,7,10,12,18	15,18	$2^{-17.5}$
$(0,0,0,0,1,0,1,0,0,1,0,1,0,0,1,1) \xrightarrow{1r} (0,0,0,0,0,1,0,0,1,0,1,0,0,0,1,0)$	5,7,10,12,16,17	15,17	2^{-23}
$(0,0,0,0,1,0,1,0,0,1,0,1,0,1,0,0) \xrightarrow{1r} (1,1,1,0,0,1,1,1,0,0,1,0,0,0,1,1)$	5,7,10,12,14,17,18	17,18	2^{-12}
$(0,0,0,0,1,0,1,0,0,1,0,1,0,1,0,1) \xrightarrow{1r} (0,0,0,1,1,0,0,0,1,1,0,1,1,1,0,1)$	5,7,10,12,14,16	—	$2^{-17.5}$
$(0,0,0,0,1,0,1,0,0,1,0,1,0,1,1,0) \xrightarrow{1r} (0,0,1,0,0,1,1,0,0,0,1,0,0,0,1,1)$	5,7,10,12,14,17	15,17	2^{-12}
$(0,0,0,0,1,0,1,0,0,1,0,1,0,1,1,1) \xrightarrow{1r} (1,1,0,1,1,0,0,1,1,1,0,1,1,1,0,1)$	5,7,10,12,14,16,18	15,18	$2^{-17.5}$
$(0,0,0,0,1,0,1,0,0,1,0,1,1,0,0,0) \xrightarrow{1r} (1,1,1,0,1,1,1,0,0,0,0,1,1,1,0,0)$	5,7,10,12,18	13,18	2^{-12}
$(0,0,0,0,1,0,1,0,0,1,0,1,1,0,0,1) \xrightarrow{1r} (0,0,0,1,0,0,0,1,1,1,1,0,0,0,1,0)$	5,7,10,12,16,17	13,17	$2^{-17.5}$
$(0,0,0,0,1,0,1,0,0,1,0,1,1,0,0,0) \xrightarrow{1r} (0,0,1,0,1,1,1,1,0,0,0,1,1,1,0,0)$	5,7,10,12	13,15	2^{-12}
$(0,0,0,0,1,0,1,0,0,1,0,1,1,0,1,1) \xrightarrow{1r} (1,1,0,1,0,0,0,0,1,1,1,0,0,0,1,0)$	5,7,10,12,16,17,18	13,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,0,1,0,0,1,0,1,1,1,0,0) \xrightarrow{1r} (0,0,1,1,0,0,1,1,0,1,1,0,0,0,1,1)$	5,7,10,12,14,17	13,17	$2^{-17.5}$
$(0,0,0,0,1,0,1,0,0,1,0,1,1,1,0,1) \xrightarrow{1r} (1,1,0,0,1,1,0,0,1,0,0,1,1,1,0,1)$	5,7,10,12,14,16,18	13,18	2^{-23}
$(0,0,0,0,1,0,1,0,0,1,0,1,1,1,1,0) \xrightarrow{1r} (1,1,1,1,0,0,1,0,0,1,1,0,0,0,1,1)$	5,7,10,12,14,17,18	13,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,0,1,0,0,1,0,1,1,1,1,1) \xrightarrow{1r} (0,0,0,0,1,1,0,1,1,0,0,1,1,1,0,1)$	5,7,10,12,14,16	13,15	2^{-23}

Table 0.84 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	5,7,10,17	11,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	5,7,10,16,18	11,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	5,7,10,17,18	11,15,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	5,7,10,16	11,15	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	5,7,10,14,18	11,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	5,7,10,14,16,17	11,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	5,7,10,14	11,15	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	5,7,10,14,16,17,18	11,15,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	5,7,10,17,18	11,13,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	5,7,10,16	11,13	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	5,7,10,17	11,13,15,17	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	5,7,10,16,18	11,13,15,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	5,7,10,14	11,13	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	5,7,10,14,16,17,18	11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	5,7,10,14,18	11,13,15,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	5,7,10,14,16,17	11,13,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	5,7,10,12,18	11,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	5,7,10,12,16,17	11,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	5,7,10,12	11,15	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	5,7,10,12,16,17,18	11,15,17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	5,7,10,12,14,17	11,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	5,7,10,12,14,16,18	11,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	5,7,10,12,14,17,18	11,15,17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	5,7,10,12,14,16	11,15	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	5,7,10,12	11,13	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	5,7,10,12,16,17,18	11,13,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	5,7,10,12,18	11,13,15,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	5,7,10,12,16,17	11,13,15,17	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	5,7,10,12,14,17,18	11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	5,7,10,12,14,16	11,13	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	5,7,10,12,14,17	11,13,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	5,7,10,12,14,16,18	11,13,15,18	2^{-23}

Table 0.85 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	5,7,18	9,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	5,7,16,17	9,17	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	5,7	9,15	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	5,7,16,17,18	9,15,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	5,7,14,17	9,17	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	5,7,14,16,18	9,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	5,7,14,17,18	9,15,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	5,7,14,16	9,15	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	5,7	9,13	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	5,7,16,17,18	9,13,17,18	2^{-34}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	5,7,18	9,13,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	5,7,16,17	9,13,15,17	2^{-34}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	5,7,14,17,18	9,13,17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	5,7,14,16	9,13	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	5,7,14,17	9,13,15,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	5,7,14,16,18	9,13,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	5,7,12,17	9,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	5,7,12,16,18	9,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	5,7,12,17,18	9,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	5,7,12,16	9,15	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	5,7,12,14,18	9,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	5,7,12,14,16,17	9,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	5,7,12,14	9,15	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	5,7,12,14,16,17,18	9,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	5,7,12,17,18	9,13,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	5,7,12,16	9,13	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	5,7,12,17	9,13,15,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	5,7,12,16,18	9,13,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	5,7,12,14	9,13	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	5,7,12,14,16,17,18	9,13,17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	5,7,12,14,18	9,13,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	5,7,12,14,16,17	9,13,15,17	2^{-23}

Table 0.86 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	5,7	9,11	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	5,7,16,17,18	9,11,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	5,7,18	9,11,15,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	5,7,16,17	9,11,15,17	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	5,7,14,17,18	9,11,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	5,7,14,16	9,11	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	5,7,14,17	9,11,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	5,7,14,16,18	9,11,15,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	5,7,18	9,11,13,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	5,7,16,17	9,11,13,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	5,7	9,11,13,15	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	5,7,16,17,18	9,11,13,15,17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	5,7,14,17	9,11,13,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	5,7,14,16,18	9,11,13,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	5,7,14,17,18	9,11,13,15,17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	5,7,14,16	9,11,13,15	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	5,7,12,17,18	9,11,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	5,7,12,16	9,11	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	5,7,12,17	9,11,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	5,7,12,16,18	9,11,15,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	5,7,12,14	9,11	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	5,7,12,14,16,17,18	9,11,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	5,7,12,14,18	9,11,15,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	5,7,12,14,16,17	9,11,15,17	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	5,7,12,17	9,11,13,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	5,7,12,16,18	9,11,13,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	5,7,12,17,18	9,11,13,15,17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	5,7,12,16	9,11,13,15	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	5,7,12,14,18	9,11,13,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	5,7,12,14,16,17	9,11,13,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	5,7,12,14	9,11,13,15	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	5,7,12,14,16,17,18	9,11,13,15,17,18	2^{-23}

Table 0.87 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,0,1,0,1,1,0,0,0,0,0,0) \xrightarrow{1r} (0,1,1,1,0,0,0,0,0,1,0,1,0,1,1,1)$	5,7,10,17	9,17	$2^{-6.5}$
$(0,0,0,0,1,0,1,0,1,1,0,0,0,0,0,1) \xrightarrow{1r} (1,0,0,0,1,1,1,1,1,0,1,0,1,0,0,1)$	5,7,10,16,18	9,18	2^{-23}
$(0,0,0,0,1,0,1,0,1,1,0,0,0,0,1,0) \xrightarrow{1r} (1,0,1,1,0,0,0,1,0,1,0,1,0,1,1,1)$	5,7,10,17,18	9,15,17,18	$2^{-6.5}$
$(0,0,0,0,1,0,1,0,1,1,0,0,0,0,1,1) \xrightarrow{1r} (0,1,0,0,1,1,1,0,1,0,1,0,1,0,0,1)$	5,7,10,16	9,15	2^{-23}
$(0,0,0,0,1,0,1,0,1,1,0,0,0,1,0,0) \xrightarrow{1r} (1,0,1,0,1,1,0,1,0,0,1,0,1,0,0,0)$	5,7,10,14,18	9,18	2^{-12}
$(0,0,0,0,1,0,1,0,1,1,0,0,0,1,0,1) \xrightarrow{1r} (0,1,0,1,0,0,1,0,1,1,0,1,0,1,1,0)$	5,7,10,14,16,17	9,17	$2^{-6.5}$
$(0,0,0,0,1,0,1,0,1,1,0,0,0,1,1,0) \xrightarrow{1r} (0,1,1,0,1,1,0,0,0,0,1,0,1,0,0,0)$	5,7,10,14	9,15	2^{-12}
$(0,0,0,0,1,0,1,0,1,1,0,0,0,1,1,1) \xrightarrow{1r} (1,0,0,1,0,0,1,1,1,1,0,1,0,1,1,0)$	5,7,10,14,16,17,18	9,15,17,18	$2^{-6.5}$
$(0,0,0,0,1,0,1,0,1,1,0,0,1,0,0,0) \xrightarrow{1r} (1,0,1,0,0,1,0,0,0,0,0,1,0,1,1,1)$	5,7,10,17,18	9,13,17,18	2^{-1}
$(0,0,0,0,1,0,1,0,1,1,0,0,1,0,0,1) \xrightarrow{1r} (0,1,0,1,1,0,1,1,1,1,0,1,0,1,0,0)$	5,7,10,16	9,13	$2^{-17.5}$
$(0,0,0,0,1,0,1,0,1,1,0,0,1,0,1,0) \xrightarrow{1r} (0,1,1,0,0,1,0,1,0,0,0,1,0,1,1,1)$	5,7,10,17	9,13,15,17	2^{-1}
$(0,0,0,0,1,0,1,0,1,1,0,0,1,0,1,1) \xrightarrow{1r} (1,0,0,1,1,0,1,0,1,1,1,1,0,1,0,0)$	5,7,10,16,18	9,13,15,18	$2^{-17.5}$
$(0,0,0,0,1,0,1,0,1,1,0,0,1,1,0,0) \xrightarrow{1r} (0,1,1,1,1,0,0,1,0,1,1,0,1,0,0,0)$	5,7,10,14	9,13	$2^{-17.5}$
$(0,0,0,0,1,0,1,0,1,1,0,0,1,1,0,1) \xrightarrow{1r} (1,0,0,0,0,1,1,0,1,0,0,1,0,1,1,0)$	5,7,10,14,16,17,18	9,13,17,18	2^{-12}
$(0,0,0,0,1,0,1,0,1,1,0,0,1,1,1,0) \xrightarrow{1r} (1,0,1,1,1,0,0,0,0,1,1,0,1,0,0,0)$	5,7,10,14,18	9,13,15,18	$2^{-17.5}$
$(0,0,0,0,1,0,1,0,1,1,0,0,1,1,1,1) \xrightarrow{1r} (0,1,0,0,0,1,1,1,1,0,0,1,0,1,1,0)$	5,7,10,14,16,17	9,13,15,17	2^{-12}
$(0,0,0,0,1,0,1,0,1,1,0,1,0,0,0,0) \xrightarrow{1r} (1,0,1,0,1,1,1,1,0,0,0,0,1,0,0,0)$	5,7,10,12,18	9,18	2^{-12}
$(0,0,0,0,1,0,1,0,1,1,0,1,0,0,0,1) \xrightarrow{1r} (0,1,0,1,0,0,0,0,1,1,1,1,0,1,1,0)$	5,7,10,12,16,17	9,17	$2^{-17.5}$
$(0,0,0,0,1,0,1,0,1,1,0,1,0,0,1,0) \xrightarrow{1r} (0,1,1,0,1,1,1,0,0,0,0,0,1,0,0,0)$	5,7,10,12	9,15	2^{-12}
$(0,0,0,0,1,0,1,0,1,1,0,1,0,0,1,1) \xrightarrow{1r} (1,0,0,1,0,0,0,1,1,1,1,1,0,1,1,0)$	5,7,10,12,16,17,18	9,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,0,1,0,1,1,0,1,0,1,0,0) \xrightarrow{1r} (0,1,1,1,0,0,1,0,0,1,1,1,0,1,1,1)$	5,7,10,12,14,17	9,17	$2^{-17.5}$
$(0,0,0,0,1,0,1,0,1,1,0,1,0,1,0,1) \xrightarrow{1r} (1,0,0,0,1,1,0,1,1,0,0,0,1,0,0,1)$	5,7,10,12,14,16,18	9,18	2^{-23}
$(0,0,0,0,1,0,1,0,1,1,0,1,0,1,1,1) \xrightarrow{1r} (1,0,1,1,0,0,1,1,0,1,1,1,0,1,1,1)$	5,7,10,12,14,17,18	9,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,0,1,0,1,1,0,1,0,1,1,1) \xrightarrow{1r} (0,1,0,0,1,1,0,0,1,0,0,0,1,0,0,1)$	5,7,10,12,14,16	9,15	2^{-23}
$(0,0,0,0,1,0,1,0,1,1,0,1,1,0,0,0) \xrightarrow{1r} (0,1,1,1,1,0,1,1,0,1,0,0,1,0,0,0)$	5,7,10,12	9,13	$2^{-17.5}$
$(0,0,0,0,1,0,1,0,1,1,0,1,1,0,0,1) \xrightarrow{1r} (1,0,0,0,0,1,0,0,1,0,1,1,0,1,1,0)$	5,7,10,12,16,17,18	9,13,17,18	2^{-23}
$(0,0,0,0,1,0,1,0,1,1,0,1,1,0,1,0) \xrightarrow{1r} (1,0,1,1,1,0,1,0,0,1,0,0,1,0,0,0)$	5,7,10,12,18	9,13,15,18	$2^{-17.5}$
$(0,0,0,0,1,0,1,0,1,1,0,1,1,0,1,1) \xrightarrow{1r} (0,1,0,0,0,1,0,1,1,0,1,1,0,1,1,0)$	5,7,10,12,16,17	9,13,15,17	2^{-23}
$(0,0,0,0,1,0,1,0,1,1,0,1,1,1,0,0) \xrightarrow{1r} (1,0,1,0,0,1,1,0,0,0,1,1,0,1,1,1)$	5,7,10,12,14,17,18	9,13,17,18	2^{-12}
$(0,0,0,0,1,0,1,0,1,1,0,1,1,1,0,1) \xrightarrow{1r} (0,1,0,1,1,0,0,1,1,1,0,0,1,0,0,1)$	5,7,10,12,14,16	9,13	$2^{-17.5}$
$(0,0,0,0,1,0,1,0,1,1,0,1,1,1,1,0) \xrightarrow{1r} (0,1,1,0,0,1,1,1,0,0,1,1,0,1,1,1)$	5,7,10,12,14,17	9,13,15,17	2^{-12}
$(0,0,0,0,1,0,1,0,1,1,0,1,1,1,1,1) \xrightarrow{1r} (1,0,0,1,1,0,0,0,1,1,0,0,1,0,0,1)$	5,7,10,12,14,16,18	9,13,15,18	$2^{-17.5}$

Table 0.88 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	5,7,10,17,18	9,11,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	5,7,10,16	9,11	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	5,7,10,17	9,11,15,17	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	5,7,10,16,18	9,11,15,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	5,7,10,14	9,11	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	5,7,10,14,16,17,18	9,11,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	5,7,10,14,18	9,11,15,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	5,7,10,14,16,17	9,11,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	5,7,10,17	9,11,13,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	5,7,10,16,18	9,11,13,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	5,7,10,17,18	9,11,13,15,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	5,7,10,16	9,11,13,15	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	5,7,10,14,18	9,11,13,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	5,7,10,14,16,17	9,11,13,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	5,7,10,14	9,11,13,15	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	5,7,10,14,16,17,18	9,11,13,15,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	5,7,10,12	9,11	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	5,7,10,12,16,17,18	9,11,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	5,7,10,12,18	9,11,15,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	5,7,10,12,16,17	9,11,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	5,7,10,12,14,17,18	9,11,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	5,7,10,12,14,16	9,11	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	5,7,10,12,14,17	9,11,15,17	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	5,7,10,12,14,16,18	9,11,15,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	5,7,10,12,18	9,11,13,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	5,7,10,12,16,17	9,11,13,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	5,7,10,12	9,11,13,15	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	5,7,10,12,16,17,18	9,11,13,15,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	5,7,10,12,14,17	9,11,13,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	5,7,10,12,14,16,18	9,11,13,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	5,7,10,12,14,17,18	9,11,13,15,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	5,7,10,12,14,16	9,11,13,15	$2^{-17.5}$

Table 0.89 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,0,1,1,0,0,0,0,0,0,0,0) \xrightarrow{1r} (1,1,1,0,1,1,1,1,1,0,1,0,1,0,0,1)$	5,7,17,18	8,17,18	2^{-23}
$(0,0,0,0,1,0,1,1,0,0,0,0,0,0,0,1) \xrightarrow{1r} (0,0,0,1,0,0,0,0,0,0,1,0,1,0,1,1)$	5,7,16	8	$2^{-6.5}$
$(0,0,0,0,1,0,1,1,0,0,0,0,0,0,1,0) \xrightarrow{1r} (0,0,1,0,1,1,1,0,1,0,1,0,1,0,0,1)$	5,7,17	8,15,17	2^{-23}
$(0,0,0,0,1,0,1,1,0,0,0,0,0,0,1,1) \xrightarrow{1r} (1,1,0,1,0,0,0,1,0,1,0,1,0,1,1,1)$	5,7,16,18	8,15,18	$2^{-6.5}$
$(0,0,0,0,1,0,1,1,0,0,0,0,0,1,0,0) \xrightarrow{1r} (0,0,1,1,0,0,1,0,1,1,1,0,1,0,1,1)$	5,7,14	8	$2^{-6.5}$
$(0,0,0,0,1,0,1,1,0,0,0,0,0,1,0,1) \xrightarrow{1r} (1,1,0,0,1,1,0,1,0,0,1,0,1,0,0,0)$	5,7,14,16,17,18	8,17,18	2^{-12}
$(0,0,0,0,1,0,1,1,0,0,0,0,0,1,1,0) \xrightarrow{1r} (1,1,1,1,0,0,1,1,1,1,0,1,0,1,1,0)$	5,7,14,18	8,15,18	$2^{-6.5}$
$(0,0,0,0,1,0,1,1,0,0,0,0,0,1,1,1) \xrightarrow{1r} (0,0,0,0,1,1,0,0,0,0,1,0,1,0,0,0)$	5,7,14,16,17	8,15,17	2^{-12}
$(0,0,0,0,1,0,1,1,0,0,0,0,0,1,0,0) \xrightarrow{1r} (0,0,1,1,1,0,1,1,1,1,1,0,1,0,0,1)$	5,7,17	8,13,17	$2^{-17.5}$
$(0,0,0,0,1,0,1,1,0,0,0,0,0,1,0,1) \xrightarrow{1r} (1,1,0,0,0,1,0,0,0,0,0,1,0,1,1,1)$	5,7,16,18	8,13,18	2^{-1}
$(0,0,0,0,1,0,1,1,0,0,0,0,0,1,0,1) \xrightarrow{1r} (1,1,1,1,1,0,1,0,1,1,1,0,1,0,0,1)$	5,7,17,18	8,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,0,1,1,0,0,0,0,0,1,0,1) \xrightarrow{1r} (0,0,0,0,0,1,0,1,0,0,0,1,0,1,1,1)$	5,7,16	8,13,15	2^{-1}
$(0,0,0,0,1,0,1,1,0,0,0,0,0,1,1,0) \xrightarrow{1r} (1,1,1,0,0,1,1,0,1,0,0,1,0,1,1,0)$	5,7,14,18	8,13,18	2^{-12}
$(0,0,0,0,1,0,1,1,0,0,0,0,0,1,1,0) \xrightarrow{1r} (0,0,0,1,1,0,0,1,0,1,1,0,1,0,0,0)$	5,7,14,16,17	8,13,17	$2^{-17.5}$
$(0,0,0,0,1,0,1,1,0,0,0,0,0,1,1,1) \xrightarrow{1r} (0,0,1,0,0,1,1,1,1,0,0,1,0,1,1,0)$	5,7,14	8,13,15	2^{-12}
$(0,0,0,0,1,0,1,1,0,0,0,0,0,1,1,1) \xrightarrow{1r} (1,1,0,1,1,0,0,0,0,1,1,0,1,0,0,0)$	5,7,14,16,17,18	8,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,0,1,1,0,0,0,0,1,0,0,0) \xrightarrow{1r} (0,0,1,1,0,0,0,0,1,1,1,1,0,1,1,0)$	5,7,12	8	$2^{-17.5}$
$(0,0,0,0,1,0,1,1,0,0,0,0,1,0,0,0) \xrightarrow{1r} (1,1,0,0,1,1,1,1,0,0,0,0,1,0,0,0)$	5,7,12,16,17,18	8,17,18	2^{-12}
$(0,0,0,0,1,0,1,1,0,0,0,0,1,0,0,1) \xrightarrow{1r} (1,1,1,1,0,0,0,0,1,1,1,1,1,0,1,1)$	5,7,12,18	8,15,18	$2^{-17.5}$
$(0,0,0,0,1,0,1,1,0,0,0,0,1,0,0,1) \xrightarrow{1r} (0,0,0,0,1,1,1,0,0,0,0,0,1,0,0,0)$	5,7,12,16,17	8,15,17	2^{-12}
$(0,0,0,0,1,0,1,1,0,0,0,0,1,0,1,0) \xrightarrow{1r} (1,1,1,0,1,1,0,1,1,0,0,0,1,0,0,1)$	5,7,12,14,17,18	8,17,18	2^{-23}
$(0,0,0,0,1,0,1,1,0,0,0,0,1,0,1,0) \xrightarrow{1r} (0,0,0,1,0,0,1,0,0,1,1,1,0,1,1,1)$	5,7,12,14,16	8	$2^{-17.5}$
$(0,0,0,0,1,0,1,1,0,0,0,0,1,0,1,1) \xrightarrow{1r} (0,0,1,0,1,1,0,0,1,0,0,0,1,0,0,1)$	5,7,12,14,17	8,15,17	2^{-23}
$(0,0,0,0,1,0,1,1,0,0,0,0,1,0,1,1) \xrightarrow{1r} (1,1,0,1,0,0,1,1,0,1,1,1,0,1,1,1)$	5,7,12,14,16,18	8,15,18	$2^{-17.5}$
$(0,0,0,0,1,0,1,1,0,0,0,0,1,1,0,0) \xrightarrow{1r} (1,1,1,0,0,1,0,0,1,0,1,0,1,1,0,1)$	5,7,12,18	8,13,18	2^{-23}
$(0,0,0,0,1,0,1,1,0,0,0,0,1,1,0,0) \xrightarrow{1r} (0,0,0,1,1,0,1,1,0,1,0,1,0,0,1,0)$	5,7,12,16,17	8,13,17	$2^{-17.5}$
$(0,0,0,0,1,0,1,1,0,0,0,0,1,1,0,1) \xrightarrow{1r} (0,0,1,0,0,1,0,1,1,0,1,1,0,1,1,0)$	5,7,12	8,13,15	2^{-23}
$(0,0,0,0,1,0,1,1,0,0,0,0,1,1,0,1) \xrightarrow{1r} (1,1,0,1,1,0,1,0,0,1,0,0,1,0,0,0)$	5,7,12,16,17,18	8,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,0,1,1,0,0,0,0,1,1,1,0) \xrightarrow{1r} (0,0,1,1,1,0,0,1,1,1,0,0,1,0,0,1)$	5,7,12,14,17	8,13,17	$2^{-17.5}$
$(0,0,0,0,1,0,1,1,0,0,0,0,1,1,1,0) \xrightarrow{1r} (1,1,0,0,0,1,1,0,0,0,0,1,1,0,1,1)$	5,7,12,14,16,18	8,13,18	2^{-12}
$(0,0,0,0,1,0,1,1,0,0,0,0,1,1,1,1) \xrightarrow{1r} (1,1,1,1,1,0,0,0,1,1,0,0,1,0,0,1)$	5,7,12,14,17,18	8,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,0,1,1,0,0,0,0,1,1,1,1) \xrightarrow{1r} (0,0,0,0,0,1,1,1,0,0,1,1,0,1,1,1)$	5,7,12,14,16	8,13,15	2^{-12}

Table 0.90 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	5,7,17	8,11,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	5,7,16,18	8,11,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	5,7,17,18	8,11,15,17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	5,7,16	8,11,15	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	5,7,14,18	8,11,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	5,7,14,16,17	8,11,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	5,7,14	8,11,15	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	5,7,14,16,17,18	8,11,15,17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	5,7,17,18	8,11,13,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	5,7,16	8,11,13	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	5,7,17	8,11,13,15,17	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	5,7,16,18	8,11,13,15,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	5,7,14	8,11,13	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	5,7,14,16,17,18	8,11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	5,7,14,18	8,11,13,15,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	5,7,14,16,17	8,11,13,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	5,7,12,18	8,11,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	5,7,12,16,17	8,11,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	5,7,12	8,11,15	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	5,7,12,16,17,18	8,11,15,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	5,7,12,14,17	8,11,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	5,7,12,14,16,18	8,11,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	5,7,12,14,17,18	8,11,15,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	5,7,12,14,16	8,11,15	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	5,7,12	8,11,13	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	5,7,12,16,17,18	8,11,13,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	5,7,12,18	8,11,13,15,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	5,7,12,16,17	8,11,13,15,17	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	5,7,12,14,17,18	8,11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	5,7,12,14,16	8,11,13	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	5,7,12,14,17	8,11,13,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	5,7,12,14,16,18	8,11,13,15,18	2^{-12}

Table 0.91 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	5,7,10	8	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	5,7,10,16,17,18	8,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	5,7,10,18	8,15,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	5,7,10,16,17	8,15,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	5,7,10,14,17,18	8,17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	5,7,10,14,16	8	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	5,7,10,14,17	8,15,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	5,7,10,14,16,18	8,15,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	5,7,10,18	8,13,18	2^{-34}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	5,7,10,16,17	8,13,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	5,7,10	8,13,15	2^{-34}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	5,7,10,16,17,18	8,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	5,7,10,14,17	8,13,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	5,7,10,14,16,18	8,13,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	5,7,10,14,17,18	8,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	5,7,10,14,16	8,13,15	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	5,7,10,12,17,18	8,17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	5,7,10,12,16	8	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	5,7,10,12,17	8,15,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	5,7,10,12,16,18	8,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	5,7,10,12,14	8	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	5,7,10,12,14,16,17,18	8,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	5,7,10,12,14,18	8,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	5,7,10,12,14,16,17	8,15,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	5,7,10,12,17	8,13,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	5,7,10,12,16,18	8,13,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	5,7,10,12,17,18	8,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	5,7,10,12,16	8,13,15	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	5,7,10,12,14,18	8,13,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	5,7,10,12,14,16,17	8,13,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	5,7,10,12,14	8,13,15	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	5,7,10,12,14,16,17,18	8,13,15,17,18	$2^{-17.5}$

Table 0.92 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	5,7,10,18	8,11,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	5,7,10,16,17	8,11,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	5,7,10	8,11,15	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	5,7,10,16,17,18	8,11,15,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	5,7,10,14,17	8,11,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	5,7,10,14,16,18	8,11,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	5,7,10,14,17,18	8,11,15,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	5,7,10,14,16	8,11,15	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	5,7,10	8,11,13	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	5,7,10,16,17,18	8,11,13,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	5,7,10,18	8,11,13,15,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	5,7,10,16,17	8,11,13,15,17	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	5,7,10,14,17,18	8,11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	5,7,10,14,16	8,11,13	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	5,7,10,14,17	8,11,13,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	5,7,10,14,16,18	8,11,13,15,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	5,7,10,12,17	8,11,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	5,7,10,12,16,18	8,11,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	5,7,10,12,17,18	8,11,15,17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	5,7,10,12,16	8,11,15	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	5,7,10,12,14,18	8,11,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	5,7,10,12,14,16,17	8,11,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	5,7,10,12,14	8,11,15	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	5,7,10,12,14,16,17,18	8,11,15,17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	5,7,10,12,17,18	8,11,13,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	5,7,10,12,16	8,11,13	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	5,7,10,12,17	8,11,13,15,17	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	5,7,10,12,16,18	8,11,13,15,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	5,7,10,12,14	8,11,13	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	5,7,10,12,14,16,17,18	8,11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	5,7,10,12,14,18	8,11,13,15,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	5,7,10,12,14,16,17	8,11,13,15,17	$2^{-17.5}$

Table 0.93 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	5,7,17	8,9,17	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	5,7,16,18	8,9,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	5,7,17,18	8,9,15,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	5,7,16	8,9,15	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	5,7,14,18	8,9,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	5,7,14,16,17	8,9,17	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	5,7,14	8,9,15	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	5,7,14,16,17,18	8,9,15,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	5,7,17,18	8,9,13,17,18	2^{-34}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	5,7,16	8,9,13	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	5,7,17	8,9,13,15,17	2^{-34}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	5,7,16,18	8,9,13,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	5,7,14	8,9,13	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	5,7,14,16,17,18	8,9,13,17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	5,7,14,18	8,9,13,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	5,7,14,16,17	8,9,13,15,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	5,7,12,18	8,9,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	5,7,12,16,17	8,9,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	5,7,12	8,9,15	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	5,7,12,16,17,18	8,9,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	5,7,12,14,17	8,9,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	5,7,12,14,16,18	8,9,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	5,7,12,14,17,18	8,9,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	5,7,12,14,16	8,9,15	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	5,7,12	8,9,13	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	5,7,12,16,17,18	8,9,13,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	5,7,12,18	8,9,13,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	5,7,12,16,17	8,9,13,15,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	5,7,12,14,17,18	8,9,13,17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	5,7,12,14,16	8,9,13	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	5,7,12,14,17	8,9,13,15,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	5,7,12,14,16,18	8,9,13,15,18	$2^{-17.5}$

Table 0.94 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	5,7,17,18	8,9,11,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	5,7,16	8,9,11	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	5,7,17	8,9,11,15,17	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	5,7,16,18	8,9,11,15,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	5,7,14	8,9,11	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	5,7,14,16,17,18	8,9,11,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	5,7,14,18	8,9,11,15,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	5,7,14,16,17	8,9,11,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	5,7,17	8,9,11,13,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	5,7,16,18	8,9,11,13,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	5,7,17,18	8,9,11,13,15,17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	5,7,16	8,9,11,13,15	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	5,7,14,18	8,9,11,13,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	5,7,14,16,17	8,9,11,13,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	5,7,14	8,9,11,13,15	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	5,7,14,16,17,18	8,9,11,13,15,17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	5,7,12	8,9,11	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	5,7,12,16,17,18	8,9,11,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	5,7,12,18	8,9,11,15,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	5,7,12,16,17	8,9,11,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	5,7,12,14,17,18	8,9,11,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	5,7,12,14,16	8,9,11	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	5,7,12,14,17	8,9,11,15,17	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	5,7,12,14,16,18	8,9,11,15,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	5,7,12,18	8,9,11,13,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	5,7,12,16,17	8,9,11,13,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	5,7,12	8,9,11,13,15	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	5,7,12,16,17,18	8,9,11,13,15,17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	5,7,12,14,17	8,9,11,13,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	5,7,12,14,16,18	8,9,11,13,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	5,7,12,14,17,18	8,9,11,13,15,17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	5,7,12,14,16	8,9,11,13,15	$2^{-17.5}$

Table 0.95 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	5,7,10,18	8,9,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	5,7,10,16,17	8,9,17	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	5,7,10	8,9,15	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	5,7,10,16,17,18	8,9,15,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	5,7,10,14,17	8,9,17	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	5,7,10,14,16,18	8,9,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	5,7,10,14,17,18	8,9,15,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	5,7,10,14,16	8,9,15	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	5,7,10	8,9,13	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	5,7,10,16,17,18	8,9,13,17,18	2^{-1}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	5,7,10,18	8,9,13,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	5,7,10,16,17	8,9,13,15,17	2^{-1}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	5,7,10,14,17,18	8,9,13,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	5,7,10,14,16	8,9,13	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	5,7,10,14,17	8,9,13,15,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	5,7,10,14,16,18	8,9,13,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	5,7,10,12,17	8,9,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	5,7,10,12,16,18	8,9,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	5,7,10,12,17,18	8,9,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	5,7,10,12,16	8,9,15	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	5,7,10,12,14,18	8,9,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	5,7,10,12,14,16,17	8,9,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	5,7,10,12,14	8,9,15	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	5,7,10,12,14,16,17,18	8,9,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	5,7,10,12,17,18	8,9,13,17,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	5,7,10,12,16	8,9,13	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	5,7,10,12,17	8,9,13,15,17	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	5,7,10,12,16,18	8,9,13,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	5,7,10,12,14	8,9,13	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	5,7,10,12,14,16,17,18	8,9,13,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	5,7,10,12,14,18	8,9,13,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	5,7,10,12,14,16,17	8,9,13,15,17	2^{-12}

Table 0.96 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	5,7,10	8,9,11	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	5,7,10,16,17,18	8,9,11,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	5,7,10,18	8,9,11,15,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	5,7,10,16,17	8,9,11,15,17	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	5,7,10,14,17,18	8,9,11,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	5,7,10,14,16	8,9,11	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	5,7,10,14,17	8,9,11,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	5,7,10,14,16,18	8,9,11,15,18	2^{-23}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	5,7,10,18	8,9,11,13,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	5,7,10,16,17	8,9,11,13,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	5,7,10	8,9,11,13,15	$2^{-28.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	5,7,10,16,17,18	8,9,11,13,15,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	5,7,10,14,17	8,9,11,13,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	5,7,10,14,16,18	8,9,11,13,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	5,7,10,14,17,18	8,9,11,13,15,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	5,7,10,14,16	8,9,11,13,15	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	5,7,10,12,17,18	8,9,11,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	5,7,10,12,16	8,9,11	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	5,7,10,12,17	8,9,11,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	5,7,10,12,16,18	8,9,11,15,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	5,7,10,12,14	8,9,11	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	5,7,10,12,14,16,17,18	8,9,11,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	5,7,10,12,14,18	8,9,11,15,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	5,7,10,12,14,16,17	8,9,11,15,17	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	5,7,10,12,17	8,9,11,13,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	5,7,10,12,16,18	8,9,11,13,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	5,7,10,12,17,18	8,9,11,13,15,17,18	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	5,7,10,12,16	8,9,11,13,15	$2^{-6.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	5,7,10,12,14,18	8,9,11,13,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	5,7,10,12,14,16,17	8,9,11,13,17	2^{-12}
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	5,7,10,12,14	8,9,11,13,15	$2^{-17.5}$
$(0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	5,7,10,12,14,16,17,18	8,9,11,13,15,17,18	2^{-12}

Table 0.97 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	5,17	6,17	2^{-12}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	5,16,18	6,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	5,17,18	6,15,17,18	2^{-12}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	5,16	6,15	$2^{-6.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	5,14,18	6,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	5,14,16,17	6,17	2^{-23}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	5,14	6,15	$2^{-6.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	5,14,16,17,18	6,15,17,18	2^{-23}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	5,17,18	6,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	5,16	6,13	2^{-12}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	5,17	6,13,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	5,16,18	6,13,15,18	2^{-12}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	5,14	6,13	2^{-1}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	5,14,16,17,18	6,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	5,14,18	6,13,15,18	2^{-1}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	5,14,16,17	6,13,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	5,12,18	6,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	5,12,16,17	6,17	2^{-23}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	5,12	6,15	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	5,12,16,17,18	6,15,17,18	2^{-23}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	5,12,14,17	6,17	2^{-12}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	5,12,14,16,18	6,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	5,12,14,17,18	6,15,17,18	2^{-12}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	5,12,14,16	6,15	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	5,12	6,13	2^{-12}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	5,12,16,17,18	6,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	5,12,18	6,13,15,18	2^{-12}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	5,12,16,17	6,13,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	5,12,14,17,18	6,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	5,12,14,16	6,13	2^{-23}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	5,12,14,17	6,13,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	5,12,14,16,18	6,13,15,18	2^{-23}

Table 0.98 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,1,0,0,0,0,1,0,0,0,0,0) \xrightarrow{1r} (1,1,0,0,1,0,1,1,0,1,1,1,0,1,1,1)$	5,17,18	6,11,17,18	2^{-23}
$(0,0,0,0,1,1,0,0,0,0,1,0,0,0,0,1) \xrightarrow{1r} (0,0,1,1,0,1,0,0,1,0,0,0,1,0,0,1)$	5,16	6,11	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,0,0,1,0,0,0,1,0) \xrightarrow{1r} (0,0,0,0,1,0,1,0,0,1,1,1,0,1,1,1)$	5,17	6,11,15,17	2^{-23}
$(0,0,0,0,1,1,0,0,0,0,1,0,0,0,1,1) \xrightarrow{1r} (1,1,1,1,0,1,0,1,1,0,0,0,1,0,0,1)$	5,16,18	6,11,15,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,0,0,1,0,0,1,0,0) \xrightarrow{1r} (0,0,0,1,0,1,1,0,0,0,0,0,1,0,0,0)$	5,14	6,11	$2^{-6.5}$
$(0,0,0,0,1,1,0,0,0,0,1,0,0,1,0,1) \xrightarrow{1r} (1,1,1,0,1,0,0,1,1,1,1,1,0,1,1,0)$	5,14,16,17,18	6,11,17,18	2^{-23}
$(0,0,0,0,1,1,0,0,0,0,1,0,0,1,1,0) \xrightarrow{1r} (1,1,0,1,0,1,1,1,0,0,0,0,1,0,0,0)$	5,14,18	6,11,15,18	$2^{-6.5}$
$(0,0,0,0,1,1,0,0,0,0,1,0,0,1,1,1) \xrightarrow{1r} (0,0,1,0,1,0,0,0,1,1,1,1,0,1,1,0)$	5,14,16,17	6,11,15,17	2^{-23}
$(0,0,0,0,1,1,0,0,0,0,1,0,1,0,0,0) \xrightarrow{1r} (0,0,0,1,1,1,1,1,0,0,1,1,0,1,1,1)$	5,17	6,11,13,17	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,0,0,1,0,1,0,0,1) \xrightarrow{1r} (1,1,1,0,0,0,0,0,1,1,0,0,1,0,0,1)$	5,16,18	6,11,13,18	2^{-12}
$(0,0,0,0,1,1,0,0,0,0,1,0,1,0,1,0) \xrightarrow{1r} (1,1,0,1,1,1,1,0,0,0,1,1,0,1,1,1)$	5,17,18	6,11,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,0,0,1,0,1,0,1,1) \xrightarrow{1r} (0,0,1,0,0,0,0,1,1,1,0,0,1,0,0,1)$	5,16	6,11,13,15	2^{-12}
$(0,0,0,0,1,1,0,0,0,0,1,0,1,1,0,0) \xrightarrow{1r} (1,1,0,0,0,0,1,0,0,1,0,0,1,0,0,0)$	5,14,18	6,11,13,18	2^{-12}
$(0,0,0,0,1,1,0,0,0,0,1,0,1,1,0,1) \xrightarrow{1r} (0,0,1,1,1,1,0,1,1,0,1,1,0,1,1,0)$	5,14,16,17	6,11,13,17	$2^{-28.5}$
$(0,0,0,0,1,1,0,0,0,0,1,0,1,1,1,0) \xrightarrow{1r} (0,0,0,0,0,0,1,1,0,1,0,0,1,0,0,0)$	5,14	6,11,13,15	2^{-12}
$(0,0,0,0,1,1,0,0,0,0,1,0,1,1,1,1) \xrightarrow{1r} (1,1,1,1,1,1,0,0,1,0,1,1,0,1,1,0)$	5,14,16,17,18	6,11,13,15,17,18	$2^{-28.5}$
$(0,0,0,0,1,1,0,0,0,0,1,1,0,0,0,0) \xrightarrow{1r} (0,0,0,1,0,1,0,0,0,0,1,0,1,0,1,0,0,0)$	5,12	6,11	$2^{-6.5}$
$(0,0,0,0,1,1,0,0,0,0,1,1,0,0,0,1) \xrightarrow{1r} (1,1,1,0,1,0,1,1,1,1,0,1,0,1,1,0)$	5,12,16,17,18	6,11,17,18	2^{-12}
$(0,0,0,0,1,1,0,0,0,0,1,1,0,0,1,0) \xrightarrow{1r} (1,1,0,1,0,1,0,1,0,0,1,0,1,0,0,0)$	5,12,18	6,11,15,18	$2^{-6.5}$
$(0,0,0,0,1,1,0,0,0,0,1,1,0,0,1,1) \xrightarrow{1r} (0,0,1,0,1,0,1,0,1,1,1,0,1,0,1,1,0)$	5,12,16,17	6,11,15,17	2^{-12}
$(0,0,0,0,1,1,0,0,0,0,1,1,0,1,0,0) \xrightarrow{1r} (1,1,0,0,1,0,0,1,0,1,0,1,0,1,1,1)$	5,12,14,17,18	6,11,17,18	2^{-12}
$(0,0,0,0,1,1,0,0,0,0,1,1,0,1,0,1) \xrightarrow{1r} (0,0,1,1,0,1,1,0,1,0,1,0,1,0,0,1)$	5,12,14,16	6,11	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,0,0,1,1,0,1,1,0) \xrightarrow{1r} (0,0,0,0,1,0,0,0,0,1,0,1,0,1,1,1)$	5,12,14,17	6,11,15,17	2^{-12}
$(0,0,0,0,1,1,0,0,0,0,1,1,0,1,1,1) \xrightarrow{1r} (1,1,1,1,0,1,1,1,1,0,1,0,1,0,0,1)$	5,12,14,16,18	6,11,15,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,0,0,1,1,1,0,0,0) \xrightarrow{1r} (1,1,0,0,0,0,0,0,0,1,1,0,1,0,0,0)$	5,12,18	6,11,13,18	2^{-12}
$(0,0,0,0,1,1,0,0,0,0,1,1,1,0,0,1) \xrightarrow{1r} (0,0,1,1,1,1,1,1,1,0,0,1,0,1,1,0)$	5,12,16,17	6,11,13,17	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,0,0,1,1,1,0,1,0) \xrightarrow{1r} (0,0,0,0,0,0,0,1,0,1,1,0,1,0,0,0)$	5,12	6,11,13,15	2^{-12}
$(0,0,0,0,1,1,0,0,0,0,1,1,1,0,1,1) \xrightarrow{1r} (1,1,1,1,1,1,1,0,1,0,0,1,0,1,1,0)$	5,12,16,17,18	6,11,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,0,0,1,1,1,1,0,0) \xrightarrow{1r} (0,0,0,1,1,1,0,1,0,0,0,1,0,1,1,1)$	5,12,14,17	6,11,13,17	$2^{-6.5}$
$(0,0,0,0,1,1,0,0,0,0,1,1,1,1,0,1) \xrightarrow{1r} (1,1,1,0,0,0,1,0,1,1,1,0,1,0,0,1)$	5,12,14,16,18	6,11,13,18	2^{-12}
$(0,0,0,0,1,1,0,0,0,0,1,1,1,1,1,0) \xrightarrow{1r} (1,1,0,1,1,1,0,0,0,0,0,1,0,1,1,1)$	5,12,14,17,18	6,11,13,15,17,18	$2^{-6.5}$
$(0,0,0,0,1,1,0,0,0,0,1,1,1,1,1,1) \xrightarrow{1r} (0,0,1,0,0,0,1,1,1,1,1,0,1,0,0,1)$	5,12,14,16	6,11,13,15	2^{-12}

Table 0.99 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	5,10,18	6,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	5,10,16,17	6,17	2^{-23}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	5,10	6,15	$2^{-28.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	5,10,16,17,18	6,15,17,18	2^{-23}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	5,10,14,17	6,17	2^{-12}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	5,10,14,16,18	6,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	5,10,14,17,18	6,15,17,18	2^{-12}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	5,10,14,16	6,15	$2^{-28.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	5,10	6,13	2^{-23}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	5,10,16,17,18	6,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	5,10,18	6,13,15,18	2^{-23}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	5,10,16,17	6,13,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	5,10,14,17,18	6,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	5,10,14,16	6,13	2^{-34}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	5,10,14,17	6,13,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	5,10,14,16,18	6,13,15,18	2^{-34}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	5,10,12,17	6,17	2^{-12}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	5,10,12,16,18	6,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	5,10,12,17,18	6,15,17,18	2^{-12}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	5,10,12,16	6,15	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	5,10,12,14,18	6,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	5,10,12,14,16,17	6,17	2^{-23}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	5,10,12,14	6,15	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	5,10,12,14,16,17,18	6,15,17,18	2^{-23}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	5,10,12,17,18	6,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	5,10,12,16	6,13	2^{-23}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	5,10,12,17	6,13,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	5,10,12,16,18	6,13,15,18	2^{-23}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	5,10,12,14	6,13	2^{-12}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	5,10,12,14,16,17,18	6,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	5,10,12,14,18	6,13,15,18	2^{-12}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	5,10,12,14,16,17	6,13,15,17	$2^{-17.5}$

Table 0.100 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	5,10	6,11	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	5,10,16,17,18	6,11,17,18	2^{-12}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	5,10,18	6,11,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	5,10,16,17	6,11,15,17	2^{-12}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	5,10,14,17,18	6,11,17,18	2^{-12}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	5,10,14,16	6,11	$2^{-28.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	5,10,14,17	6,11,15,17	2^{-12}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	5,10,14,16,18	6,11,15,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	5,10,18	6,11,13,18	2^{-23}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	5,10,16,17	6,11,13,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	5,10	6,11,13,15	2^{-23}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	5,10,16,17,18	6,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	5,10,14,17	6,11,13,17	$2^{-6.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	5,10,14,16,18	6,11,13,18	2^{-23}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	5,10,14,17,18	6,11,13,15,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	5,10,14,16	6,11,13,15	2^{-23}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	5,10,12,17,18	6,11,17,18	2^{-23}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	5,10,12,16	6,11	$2^{-28.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	5,10,12,17	6,11,15,17	2^{-23}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	5,10,12,16,18	6,11,15,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	5,10,12,14	6,11	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	5,10,12,14,16,17,18	6,11,17,18	2^{-23}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	5,10,12,14,18	6,11,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	5,10,12,14,16,17	6,11,15,17	2^{-23}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	5,10,12,17	6,11,13,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	5,10,12,16,18	6,11,13,18	2^{-23}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	5,10,12,17,18	6,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	5,10,12,16	6,11,13,15	2^{-23}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	5,10,12,14,18	6,11,13,18	2^{-23}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	5,10,12,14,16,17	6,11,13,17	$2^{-28.5}$
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	5,10,12,14	6,11,13,15	2^{-23}
$(0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	5,10,12,14,16,17,18	6,11,13,15,17,18	$2^{-28.5}$

Table 0.101 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,1,0,0,1,0,0,0,0,0,0,0) \xrightarrow{1r} (1,0,0,1,1,0,1,0,0,1,1,1,0,0,1,1)$	5,17,18	6,9,17,18	$2^{-28.5}$
$(0,0,0,0,1,1,0,0,1,0,0,0,0,0,0,1) \xrightarrow{1r} (0,1,1,0,0,1,0,1,1,0,0,0,1,1,0,1)$	5,16	6,9	2^{-23}
$(0,0,0,0,1,1,0,0,1,0,0,0,0,0,1,0) \xrightarrow{1r} (0,1,0,1,1,0,1,1,0,1,1,1,0,0,1,1)$	5,17	6,9,15,17	$2^{-28.5}$
$(0,0,0,0,1,1,0,0,1,0,0,0,0,0,1,1) \xrightarrow{1r} (1,0,1,0,0,1,0,0,1,0,0,0,1,1,0,1)$	5,16,18	6,9,15,18	2^{-23}
$(0,0,0,0,1,1,0,0,1,0,0,0,0,1,0,0) \xrightarrow{1r} (0,1,0,0,0,1,1,1,0,0,0,0,1,1,0,0)$	5,14	6,9	2^{-12}
$(0,0,0,0,1,1,0,0,1,0,0,0,0,1,0,1) \xrightarrow{1r} (1,0,1,1,1,0,0,0,1,1,1,1,0,0,1,0)$	5,14,16,17,18	6,9,17,18	$2^{-28.5}$
$(0,0,0,0,1,1,0,0,1,0,0,0,0,1,1,0) \xrightarrow{1r} (1,0,0,0,0,1,1,0,0,0,0,0,1,1,0,0)$	5,14,18	6,9,15,18	2^{-12}
$(0,0,0,0,1,1,0,0,1,0,0,0,0,1,1,1) \xrightarrow{1r} (0,1,1,1,1,0,0,1,1,1,1,1,0,0,1,0)$	5,14,16,17	6,9,15,17	$2^{-28.5}$
$(0,0,0,0,1,1,0,0,1,0,0,0,1,0,0,0) \xrightarrow{1r} (0,1,0,0,1,1,1,0,0,0,1,1,0,0,1,1)$	5,17	6,9,13,17	2^{-23}
$(0,0,0,0,1,1,0,0,1,0,0,0,1,0,0,1) \xrightarrow{1r} (1,0,1,1,0,0,0,1,1,1,0,0,1,1,0,1)$	5,16,18	6,9,13,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,0,0,0,1,0,1,0) \xrightarrow{1r} (1,0,0,0,1,1,1,1,0,0,1,1,0,0,1,1)$	5,17,18	6,9,13,15,17,18	2^{-23}
$(0,0,0,0,1,1,0,0,1,0,0,0,1,0,1,1) \xrightarrow{1r} (0,1,1,1,0,0,0,1,1,1,0,0,1,1,0,1)$	5,16	6,9,13,15	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,0,0,0,1,1,0,0) \xrightarrow{1r} (1,0,0,1,0,0,1,1,0,1,0,0,1,1,0,0)$	5,14,18	6,9,13,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,0,0,0,1,1,0,1) \xrightarrow{1r} (0,1,1,0,1,1,0,0,1,0,1,1,0,0,1,0)$	5,14,16,17	6,9,13,17	2^{-34}
$(0,0,0,0,1,1,0,0,1,0,0,0,1,1,1,0) \xrightarrow{1r} (0,1,0,1,0,0,1,0,0,1,0,0,1,1,0,0)$	5,14	6,9,13,15	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,0,0,0,1,1,1,1) \xrightarrow{1r} (1,0,1,0,1,1,0,1,1,0,1,1,0,0,1,0)$	5,14,16,17,18	6,9,13,15,17,18	2^{-34}
$(0,0,0,0,1,1,0,0,1,0,0,1,0,0,0,0) \xrightarrow{1r} (0,1,0,0,0,1,0,1,0,0,1,0,1,1,0,0)$	5,12	6,9	2^{-12}
$(0,0,0,0,1,1,0,0,1,0,0,1,0,0,0,1) \xrightarrow{1r} (1,0,1,1,1,0,1,0,1,1,0,1,0,0,1,0)$	5,12,16,17,18	6,9,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,0,0,1,0,0,1,0) \xrightarrow{1r} (1,0,0,0,0,1,0,0,0,0,1,0,1,1,0,0)$	5,12,18	6,9,15,18	2^{-12}
$(0,0,0,0,1,1,0,0,1,0,0,1,0,0,1,1) \xrightarrow{1r} (0,1,1,1,1,0,1,1,1,1,0,1,0,0,1,0)$	5,12,16,17	6,9,15,17	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,0,0,1,0,1,0,0) \xrightarrow{1r} (1,0,0,1,1,0,0,0,0,1,0,1,0,0,1,1)$	5,12,14,17,18	6,9,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,0,0,1,0,1,0,1) \xrightarrow{1r} (0,1,1,0,0,1,1,1,1,0,1,0,1,1,0,1)$	5,12,14,16	6,9	2^{-23}
$(0,0,0,0,1,1,0,0,1,0,0,1,0,1,1,0) \xrightarrow{1r} (0,1,0,1,1,0,0,1,0,1,0,1,0,0,1,1)$	5,12,14,17	6,9,15,17	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,0,0,1,0,1,1,1) \xrightarrow{1r} (1,0,1,0,0,1,1,0,1,0,1,0,1,1,0,1)$	5,12,14,16,18	6,9,15,18	2^{-23}
$(0,0,0,0,1,1,0,0,1,0,0,1,1,0,0,0) \xrightarrow{1r} (1,0,0,1,0,0,0,1,0,1,1,0,1,1,0,0)$	5,12,18	6,9,13,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,0,0,1,1,0,0,1) \xrightarrow{1r} (0,1,1,0,1,1,1,0,1,0,0,1,0,0,1,0)$	5,12,16,17	6,9,13,17	2^{-23}
$(0,0,0,0,1,1,0,0,1,0,0,1,1,0,1,0) \xrightarrow{1r} (0,1,0,1,0,0,0,0,0,1,1,0,1,1,0,0)$	5,12	6,9,13,15	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,0,0,1,1,0,1,1) \xrightarrow{1r} (1,0,1,0,1,1,1,1,1,0,0,1,0,0,1,0)$	5,12,16,17,18	6,9,13,15,17,18	2^{-23}
$(0,0,0,0,1,1,0,0,1,0,0,1,1,1,0,0) \xrightarrow{1r} (0,1,0,0,1,1,0,0,0,0,0,1,0,0,1,1)$	5,12,14,17	6,9,13,17	2^{-12}
$(0,0,0,0,1,1,0,0,1,0,0,1,1,1,0,1) \xrightarrow{1r} (1,0,1,1,0,0,1,1,1,1,1,0,1,1,0,1)$	5,12,14,16,18	6,9,13,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,0,0,1,1,1,1,0) \xrightarrow{1r} (1,0,0,0,1,1,0,1,0,0,0,1,0,0,1,1)$	5,12,14,17,18	6,9,13,15,17,18	2^{-12}
$(0,0,0,0,1,1,0,0,1,0,0,1,1,1,1,1) \xrightarrow{1r} (0,1,1,1,0,0,1,0,1,1,1,0,1,1,0,1)$	5,12,14,16	6,9,13,15	$2^{-17.5}$

Table 0.102 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,1,0,0,1,0,1,0,0,0,0,0) \xrightarrow{1r} (0,1,0,1,1,1,1,0,0,0,1,0,0,0,1,1)$	5,17	6,9,11,17	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,0,1,0,0,0,0,1) \xrightarrow{1r} (1,0,1,0,0,0,0,1,1,1,0,1,1,1,0,1)$	5,16,18	6,9,11,18	2^{-12}
$(0,0,0,0,1,1,0,0,1,0,1,0,0,0,1,0) \xrightarrow{1r} (1,0,0,1,1,1,1,1,0,0,1,0,0,0,1,1)$	5,17,18	6,9,11,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,0,1,0,0,0,1,1) \xrightarrow{1r} (0,1,1,0,0,0,0,0,1,1,0,1,1,1,0,1)$	5,16	6,9,11,15	2^{-12}
$(0,0,0,0,1,1,0,0,1,0,1,0,0,1,0,0) \xrightarrow{1r} (1,0,0,0,0,0,1,1,0,1,0,1,1,1,0,0)$	5,14,18	6,9,11,18	2^{-12}
$(0,0,0,0,1,1,0,0,1,0,1,0,0,1,0,1) \xrightarrow{1r} (0,1,1,1,1,0,0,1,0,1,0,0,0,0,1,0)$	5,14,16,17	6,9,11,17	$2^{-28.5}$
$(0,0,0,0,1,1,0,0,1,0,1,0,0,1,1,0) \xrightarrow{1r} (0,1,0,0,0,0,1,0,0,1,0,1,1,1,0,0)$	5,14	6,9,11,15	2^{-12}
$(0,0,0,0,1,1,0,0,1,0,1,0,0,1,1,1) \xrightarrow{1r} (1,0,1,1,1,1,0,1,1,0,1,0,0,0,1,0)$	5,14,16,17,18	6,9,11,15,17,18	$2^{-28.5}$
$(0,0,0,0,1,1,0,0,1,0,1,0,1,0,0,0) \xrightarrow{1r} (1,0,0,0,1,0,1,0,0,1,1,0,0,0,1,1)$	5,17,18	6,9,11,13,17,18	2^{-23}
$(0,0,0,0,1,1,0,0,1,0,1,0,1,0,0,1) \xrightarrow{1r} (0,1,1,1,0,1,0,1,1,0,0,1,1,1,0,1)$	5,16	6,9,11,13	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,0,1,0,1,0,1,0) \xrightarrow{1r} (0,1,0,0,1,0,1,1,0,1,1,0,0,0,1,1)$	5,17	6,9,11,13,15,17	2^{-23}
$(0,0,0,0,1,1,0,0,1,0,1,0,1,0,1,1) \xrightarrow{1r} (1,0,1,1,0,1,0,0,1,0,0,1,1,1,0,1)$	5,16,18	6,9,11,13,15,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,0,1,0,1,1,0,0) \xrightarrow{1r} (0,1,0,1,0,1,1,1,0,0,0,1,1,1,0,0)$	5,14	6,9,11,13	$2^{-6.5}$
$(0,0,0,0,1,1,0,0,1,0,1,0,1,1,0,1) \xrightarrow{1r} (1,0,1,0,1,0,0,0,1,1,1,0,0,0,1,0)$	5,14,16,17,18	6,9,11,13,17,18	2^{-23}
$(0,0,0,0,1,1,0,0,1,0,1,0,1,1,1,0) \xrightarrow{1r} (1,0,0,1,0,1,1,0,0,0,0,1,1,1,0,0)$	5,14,18	6,9,11,13,15,18	$2^{-6.5}$
$(0,0,0,0,1,1,0,0,1,0,1,0,1,1,1,1) \xrightarrow{1r} (0,1,1,0,1,0,0,1,1,1,1,0,0,0,1,0)$	5,14,16,17	6,9,11,13,15,17	2^{-23}
$(0,0,0,0,1,1,0,0,1,0,1,1,0,0,0,0) \xrightarrow{1r} (1,0,0,0,0,0,0,1,0,1,1,1,1,1,0,0)$	5,12,18	6,9,11,18	2^{-23}
$(0,0,0,0,1,1,0,0,1,0,1,1,0,0,0,1) \xrightarrow{1r} (0,1,1,1,1,1,0,1,0,0,0,0,0,0,1,0)$	5,12,16,17	6,9,11,17	$2^{-28.5}$
$(0,0,0,0,1,1,0,0,1,0,1,1,0,0,1,0) \xrightarrow{1r} (0,1,0,0,0,0,0,0,0,1,1,1,1,1,0,0)$	5,12	6,9,11,15	2^{-23}
$(0,0,0,0,1,1,0,0,1,0,1,1,0,0,1,1) \xrightarrow{1r} (1,0,1,1,1,1,1,1,0,0,0,0,0,0,1,0)$	5,12,16,17,18	6,9,11,15,17,18	$2^{-28.5}$
$(0,0,0,0,1,1,0,0,1,0,1,1,0,1,0,0) \xrightarrow{1r} (0,1,0,1,1,1,0,0,0,0,0,0,0,0,1,1)$	5,12,14,17	6,9,11,17	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,0,1,1,0,1,0,1) \xrightarrow{1r} (1,0,1,0,0,0,1,1,1,1,1,1,1,1,0,1)$	5,12,14,16,18	6,9,11,18	2^{-23}
$(0,0,0,0,1,1,0,0,1,0,1,1,0,1,1,0) \xrightarrow{1r} (1,0,0,1,1,1,0,1,0,0,0,0,0,0,1,1)$	5,12,14,17,18	6,9,11,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,0,1,1,0,1,1,1) \xrightarrow{1r} (0,1,1,0,0,0,1,0,1,1,1,1,1,1,0,1)$	5,12,14,16	6,9,11,15	2^{-23}
$(0,0,0,0,1,1,0,0,1,0,1,1,1,0,0,0) \xrightarrow{1r} (0,1,0,1,0,1,0,1,0,0,1,1,1,1,0,0)$	5,12	6,9,11,13	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,0,1,1,1,0,0,1) \xrightarrow{1r} (1,0,1,0,1,0,1,0,1,1,1,0,0,0,0,1,0)$	5,12,16,17,18	6,9,11,13,17,18	2^{-23}
$(0,0,0,0,1,1,0,0,1,0,1,1,1,0,1,0) \xrightarrow{1r} (1,0,0,1,0,1,0,0,0,0,1,1,1,1,0,0)$	5,12,18	6,9,11,13,15,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,0,1,1,1,0,1,1) \xrightarrow{1r} (0,1,1,0,1,0,1,1,1,1,0,0,0,0,1,0)$	5,12,16,17	6,9,11,13,15,17	2^{-23}
$(0,0,0,0,1,1,0,0,1,0,1,1,1,1,0,0) \xrightarrow{1r} (1,0,0,0,1,0,0,0,0,1,0,0,0,0,1,1)$	5,12,14,17,18	6,9,11,13,17,18	2^{-23}
$(0,0,0,0,1,1,0,0,1,0,1,1,1,1,0,1) \xrightarrow{1r} (0,1,1,1,0,1,1,1,1,0,1,1,1,1,0,1)$	5,12,14,16	6,9,11,13	$2^{-28.5}$
$(0,0,0,0,1,1,0,0,1,0,1,1,1,1,1,0) \xrightarrow{1r} (0,1,0,0,1,0,0,1,0,1,0,0,0,0,1,1)$	5,12,14,17	6,9,11,13,15,17	2^{-23}
$(0,0,0,0,1,1,0,0,1,0,1,1,1,1,1,1) \xrightarrow{1r} (1,0,1,1,0,1,1,0,1,0,1,1,1,1,0,1)$	5,12,14,16,18	6,9,11,13,15,18	$2^{-28.5}$

Table 0.103 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,1,0,0,1,1,0,0,0,0,0,0) \xrightarrow{1r} (0,1,1,0,1,1,1,1,0,0,1,0,0,1,0,0)$	5,10	6,9	2^{-12}
$(0,0,0,0,1,1,0,0,1,1,0,0,0,0,0,1) \xrightarrow{1r} (1,0,0,1,0,0,0,0,1,1,0,1,1,0,1,0)$	5,10,16,17,18	6,9,17,18	$2^{-6.5}$
$(0,0,0,0,1,1,0,0,1,1,0,0,0,0,1,0) \xrightarrow{1r} (1,0,1,0,1,1,1,0,0,0,1,0,0,1,0,0)$	5,10,18	6,9,15,18	2^{-12}
$(0,0,0,0,1,1,0,0,1,1,0,0,0,0,1,1) \xrightarrow{1r} (0,1,0,1,0,0,0,1,1,1,0,1,1,0,1,0)$	5,10,16,17	6,9,15,17	$2^{-6.5}$
$(0,0,0,0,1,1,0,0,1,1,0,0,0,1,0,0) \xrightarrow{1r} (1,0,1,1,0,0,1,0,0,1,0,1,1,0,1,1)$	5,10,14,17,18	6,9,17,18	$2^{-6.5}$
$(0,0,0,0,1,1,0,0,1,1,0,0,0,1,0,1) \xrightarrow{1r} (0,1,0,0,1,1,0,1,1,0,1,0,0,1,0,1)$	5,10,14,16	6,9	2^{-23}
$(0,0,0,0,1,1,0,0,1,1,0,0,0,1,1,0) \xrightarrow{1r} (0,1,1,1,0,0,1,1,0,1,0,1,1,0,1,1)$	5,10,14,17	6,9,15,17	$2^{-6.5}$
$(0,0,0,0,1,1,0,0,1,1,0,0,0,1,1,1) \xrightarrow{1r} (1,0,0,0,1,1,0,0,1,0,1,0,0,1,0,1)$	5,10,14,16,18	6,9,15,18	2^{-23}
$(0,0,0,0,1,1,0,0,1,1,0,0,1,0,0,0) \xrightarrow{1r} (1,0,1,1,1,0,1,1,0,1,1,0,0,1,0,0)$	5,10,18	6,9,13,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,1,0,0,1,0,0,1) \xrightarrow{1r} (0,1,0,0,0,1,0,0,1,0,0,1,1,0,1,0)$	5,10,16,17	6,9,13,17	2^{-12}
$(0,0,0,0,1,1,0,0,1,1,0,0,1,0,1,0) \xrightarrow{1r} (0,1,1,1,1,0,1,0,0,1,1,0,0,1,0,0)$	5,10	6,9,13,15	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,1,0,0,1,0,1,1) \xrightarrow{1r} (1,0,0,0,0,1,0,1,1,0,0,1,1,0,1,0)$	5,10,16,17,18	6,9,13,15,17,18	2^{-12}
$(0,0,0,0,1,1,0,0,1,1,0,0,1,1,0,0) \xrightarrow{1r} (0,1,1,0,0,1,1,0,0,0,0,1,1,0,1,1)$	5,10,14,17	6,9,13,17	2^{-1}
$(0,0,0,0,1,1,0,0,1,1,0,0,1,1,0,1) \xrightarrow{1r} (1,0,0,1,1,0,0,1,1,1,1,0,0,1,0,1)$	5,10,14,16,18	6,9,13,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,1,0,0,1,1,1,0) \xrightarrow{1r} (1,0,1,0,0,1,1,1,0,0,0,1,1,0,1,1)$	5,10,14,17,18	6,9,13,15,17,18	2^{-1}
$(0,0,0,0,1,1,0,0,1,1,0,0,1,1,1,1) \xrightarrow{1r} (0,1,0,1,1,0,0,0,1,1,1,0,0,1,0,1)$	5,10,14,16	6,9,13,15	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,1,0,1,0,0,0,0) \xrightarrow{1r} (1,0,1,1,0,0,0,0,0,1,1,1,1,0,1,1)$	5,10,12,17,18	6,9,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,1,0,1,0,0,0,1) \xrightarrow{1r} (0,1,0,0,1,1,1,1,1,0,0,0,0,1,0,1)$	5,10,12,16	6,9	2^{-23}
$(0,0,0,0,1,1,0,0,1,1,0,1,0,0,1,0) \xrightarrow{1r} (0,1,1,1,0,0,0,1,0,1,1,1,1,0,1,1)$	5,10,12,17	6,9,15,17	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,1,0,1,0,0,1,1) \xrightarrow{1r} (1,0,0,0,1,1,1,0,1,0,0,0,0,1,0,1)$	5,10,12,16,18	6,9,15,18	2^{-23}
$(0,0,0,0,1,1,0,0,1,1,0,1,0,1,0,0) \xrightarrow{1r} (0,1,1,0,1,1,0,1,0,0,0,0,0,1,0,0)$	5,10,12,14	6,9	2^{-12}
$(0,0,0,0,1,1,0,0,1,1,0,1,0,1,0,1) \xrightarrow{1r} (1,0,0,1,0,0,1,0,1,1,1,1,1,0,1,0)$	5,10,12,14,16,17,18	6,9,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,1,0,1,0,1,1,0) \xrightarrow{1r} (1,0,1,0,1,1,0,0,0,0,0,0,0,1,0,0)$	5,10,12,14,18	6,9,15,18	2^{-12}
$(0,0,0,0,1,1,0,0,1,1,0,1,0,1,1,1) \xrightarrow{1r} (0,1,0,1,0,0,1,1,1,1,1,1,1,0,1,0)$	5,10,12,14,16,17	6,9,15,17	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,1,0,1,1,0,0,0) \xrightarrow{1r} (0,1,1,0,0,1,0,0,0,0,1,1,1,0,1,1)$	5,10,12,17	6,9,13,17	2^{-12}
$(0,0,0,0,1,1,0,0,1,1,0,1,1,0,0,1) \xrightarrow{1r} (1,0,0,1,1,0,1,1,1,1,1,0,0,0,1,0,1)$	5,10,12,16,18	6,9,13,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,1,0,1,1,0,1,0) \xrightarrow{1r} (1,0,1,0,0,1,0,1,0,0,0,1,1,1,0,1,1)$	5,10,12,17,18	6,9,13,15,17,18	2^{-12}
$(0,0,0,0,1,1,0,0,1,1,0,1,1,0,1,1) \xrightarrow{1r} (0,1,0,1,1,0,1,0,1,1,0,0,0,1,0,1)$	5,10,12,16	6,9,13,15	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,1,0,1,1,1,0,0) \xrightarrow{1r} (1,0,1,1,1,0,0,1,0,1,0,0,0,0,1,0,0)$	5,10,12,14,18	6,9,13,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,1,0,1,1,1,0,1) \xrightarrow{1r} (0,1,0,0,0,1,1,0,1,0,1,1,1,0,1,0)$	5,10,12,14,16,17	6,9,13,17	2^{-23}
$(0,0,0,0,1,1,0,0,1,1,0,1,1,1,1,0) \xrightarrow{1r} (0,1,1,1,1,0,0,0,0,1,0,0,0,1,0,0)$	5,10,12,14	6,9,13,15	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,1,0,1,1,1,1,1) \xrightarrow{1r} (1,0,0,0,0,1,1,1,1,0,1,1,1,0,1,0)$	5,10,12,14,16,17,18	6,9,13,15,17,18	2^{-23}

Table 0.104 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,1,0,0,1,1,1,0,0,0,0,0) \xrightarrow{1r} (1,0,1,0,1,0,1,1,0,1,1,1,0,1,0,0)$	5,10,18	6,9,11,18	2^{-23}
$(0,0,0,0,1,1,0,0,1,1,1,0,0,0,0,1) \xrightarrow{1r} (0,1,0,1,0,1,0,0,1,0,0,0,1,0,1,0)$	5,10,16,17	6,9,11,17	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,1,1,0,0,0,1,0) \xrightarrow{1r} (0,1,1,0,1,0,1,0,0,1,1,1,0,1,0,0)$	5,10	6,9,11,15	2^{-23}
$(0,0,0,0,1,1,0,0,1,1,1,0,0,0,1,1) \xrightarrow{1r} (1,0,0,1,0,1,0,1,1,0,0,0,1,0,1,0)$	5,10,16,17,18	6,9,11,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,1,1,0,0,1,0,0) \xrightarrow{1r} (0,1,1,1,0,1,1,0,0,0,0,0,1,0,1,1)$	5,10,14,17	6,9,11,17	$2^{-6.5}$
$(0,0,0,0,1,1,0,0,1,1,1,0,0,1,0,1) \xrightarrow{1r} (1,0,0,0,1,0,0,1,1,1,1,1,0,1,0,1)$	5,10,14,16,18	6,9,11,18	2^{-23}
$(0,0,0,0,1,1,0,0,1,1,1,0,0,1,1,0) \xrightarrow{1r} (1,0,1,1,0,1,1,1,0,0,0,0,1,0,1,1)$	5,10,14,17,18	6,9,11,15,17,18	$2^{-6.5}$
$(0,0,0,0,1,1,0,0,1,1,1,0,0,1,1,1) \xrightarrow{1r} (0,1,0,0,1,0,0,0,1,1,1,1,0,1,0,1)$	5,10,14,16	6,9,11,15	2^{-23}
$(0,0,0,0,1,1,0,0,1,1,1,0,1,0,0,0) \xrightarrow{1r} (0,1,1,1,1,1,1,0,0,1,1,0,1,0,0,0)$	5,10	6,9,11,13	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,1,1,0,1,0,0,1) \xrightarrow{1r} (1,0,0,0,0,0,0,0,1,1,0,0,1,0,1,0)$	5,10,16,17,18	6,9,11,13,17,18	2^{-12}
$(0,0,0,0,1,1,0,0,1,1,1,0,1,0,1,0) \xrightarrow{1r} (1,0,1,1,1,1,1,0,0,0,1,1,0,1,0,0)$	5,10,18	6,9,11,13,15,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,1,1,0,1,0,1,1) \xrightarrow{1r} (0,1,0,0,0,0,0,1,1,1,0,0,1,0,1,0)$	5,10,16,17	6,9,11,13,15,17	2^{-12}
$(0,0,0,0,1,1,0,0,1,1,1,0,1,1,0,0) \xrightarrow{1r} (1,0,1,0,0,0,1,0,0,1,0,0,1,0,1,1)$	5,10,14,17,18	6,9,11,13,17,18	2^{-12}
$(0,0,0,0,1,1,0,0,1,1,1,0,1,1,0,1) \xrightarrow{1r} (0,1,0,1,1,1,0,1,1,0,1,1,0,1,0,1)$	5,10,14,16	6,9,11,13	$2^{-28.5}$
$(0,0,0,0,1,1,0,0,1,1,1,0,1,1,1,0) \xrightarrow{1r} (0,1,1,0,0,0,1,1,0,1,0,0,1,0,1,1)$	5,10,14,17	6,9,11,13,15,17	2^{-12}
$(0,0,0,0,1,1,0,0,1,1,1,0,1,1,1,1) \xrightarrow{1r} (1,0,0,1,1,1,0,0,1,0,1,1,0,1,0,1)$	5,10,14,16,18	6,9,11,13,15,18	$2^{-28.5}$
$(0,0,0,0,1,1,0,0,1,1,1,1,0,0,0,0) \xrightarrow{1r} (0,1,1,1,0,1,0,0,0,0,1,0,1,0,1,1)$	5,10,12,17	6,9,11,17	$2^{-6.5}$
$(0,0,0,0,1,1,0,0,1,1,1,1,0,0,0,1) \xrightarrow{1r} (1,0,0,0,1,0,1,1,1,1,0,1,0,1,0,1)$	5,10,12,16,18	6,9,11,18	2^{-12}
$(0,0,0,0,1,1,0,0,1,1,1,1,0,0,1,0) \xrightarrow{1r} (1,0,1,1,0,1,0,1,0,0,1,0,1,0,1,1)$	5,10,12,17,18	6,9,11,15,17,18	$2^{-6.5}$
$(0,0,0,0,1,1,0,0,1,1,1,1,0,0,1,1) \xrightarrow{1r} (0,1,0,0,1,0,1,0,1,1,1,0,1,0,1,0)$	5,10,12,16	6,9,11,15	2^{-12}
$(0,0,0,0,1,1,0,0,1,1,1,1,0,1,0,0) \xrightarrow{1r} (1,0,1,0,1,0,0,1,0,1,0,1,0,1,0,0)$	5,10,12,14,18	6,9,11,18	2^{-12}
$(0,0,0,0,1,1,0,0,1,1,1,1,0,1,0,1) \xrightarrow{1r} (0,1,0,1,0,1,1,0,1,0,1,0,1,0,1,0)$	5,10,12,14,16,17	6,9,11,17	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,1,1,1,0,1,1,0) \xrightarrow{1r} (0,1,1,0,1,0,0,0,0,1,0,1,0,1,0,0)$	5,10,12,14	6,9,11,15	2^{-12}
$(0,0,0,0,1,1,0,0,1,1,1,1,0,1,1,1) \xrightarrow{1r} (1,0,0,1,0,1,1,1,1,0,1,0,1,0,1,0)$	5,10,12,14,16,17,18	6,9,11,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,1,1,1,1,0,0,0) \xrightarrow{1r} (1,0,1,0,0,0,0,0,0,0,1,1,0,1,0,1)$	5,10,12,17,18	6,9,11,13,17,18	2^{-12}
$(0,0,0,0,1,1,0,0,1,1,1,1,1,0,0,1) \xrightarrow{1r} (0,1,0,1,1,1,1,1,1,0,0,1,0,1,0,1)$	5,10,12,16	6,9,11,13	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,1,1,1,1,0,1,0) \xrightarrow{1r} (0,1,1,0,0,0,0,1,0,1,1,0,1,0,1,1)$	5,10,12,17	6,9,11,13,15,17	2^{-12}
$(0,0,0,0,1,1,0,0,1,1,1,1,1,0,1,1) \xrightarrow{1r} (1,0,0,1,1,1,1,0,1,0,0,1,0,1,0,1)$	5,10,12,16,18	6,9,11,13,15,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,0,1,1,1,1,1,1,0,0) \xrightarrow{1r} (0,1,1,1,1,1,0,1,0,0,0,1,0,1,0,0)$	5,10,12,14	6,9,11,13	$2^{-6.5}$
$(0,0,0,0,1,1,0,0,1,1,1,1,1,1,0,1) \xrightarrow{1r} (1,0,0,0,0,0,1,0,1,1,1,0,1,0,1,0)$	5,10,12,14,16,17,18	6,9,11,13,17,18	2^{-12}
$(0,0,0,0,1,1,0,0,1,1,1,1,1,1,1,0) \xrightarrow{1r} (1,0,1,1,1,1,0,0,0,0,0,1,0,1,0,0)$	5,10,12,14,18	6,9,11,13,15,18	$2^{-6.5}$
$(0,0,0,0,1,1,0,0,1,1,1,1,1,1,1,1) \xrightarrow{1r} (0,1,0,0,0,0,1,1,1,1,1,0,1,0,1,0)$	5,10,12,14,16,17	6,9,11,13,15,17	2^{-12}

Table 0.105 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,1,0,1,0,0,0,0,0,0,0,0) \xrightarrow{1r} (1,1,1,1,0,0,0,0,1,1,0,1,1,0,1,0)$	5,18	6,8,18	$2^{-6.5}$
$(0,0,0,0,1,1,0,1,0,0,0,0,0,0,0,1) \xrightarrow{1r} (0,0,0,0,1,1,1,1,0,0,1,0,0,1,0,0)$	5,16,17	6,8,17	2^{-12}
$(0,0,0,0,1,1,0,1,0,0,0,0,0,0,1,0) \xrightarrow{1r} (0,0,1,1,0,0,0,1,1,1,0,1,1,0,1,0)$	5	6,8,15	$2^{-6.5}$
$(0,0,0,0,1,1,0,1,0,0,0,0,0,0,1,1) \xrightarrow{1r} (1,1,0,0,1,1,1,0,0,0,1,0,0,1,0,0)$	5,16,17,18	6,8,15,17,18	2^{-12}
$(0,0,0,0,1,1,0,1,0,0,0,0,0,1,0,0) \xrightarrow{1r} (0,0,1,0,1,1,0,1,1,0,1,0,1,0,0,1)$	5,14,17	6,8,17	2^{-23}
$(0,0,0,0,1,1,0,1,0,0,0,0,0,1,0,1) \xrightarrow{1r} (1,1,0,1,0,0,1,0,0,1,0,1,1,0,1,1)$	5,14,16,18	6,8,18	$2^{-6.5}$
$(0,0,0,0,1,1,0,1,0,0,0,0,0,1,1,0) \xrightarrow{1r} (1,1,1,0,1,1,0,0,1,0,1,0,0,1,0,1)$	5,14,17,18	6,8,15,17,18	2^{-23}
$(0,0,0,0,1,1,0,1,0,0,0,0,0,1,1,1) \xrightarrow{1r} (0,0,0,1,0,0,1,1,0,1,0,1,1,0,1,1)$	5,14,16	6,8,15	$2^{-6.5}$
$(0,0,0,0,1,1,0,1,0,0,0,0,1,0,0,0) \xrightarrow{1r} (0,0,1,0,0,1,0,0,1,0,0,1,1,0,1,0)$	5	6,8,13	2^{-12}
$(0,0,0,0,1,1,0,1,0,0,0,0,1,0,0,1) \xrightarrow{1r} (1,1,0,1,1,0,1,1,0,1,1,0,0,1,0,0)$	5,16,17,18	6,8,13,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,0,0,0,1,0,1,0) \xrightarrow{1r} (1,1,1,0,0,1,0,1,1,0,1,0,1,1,0,1)$	5,18	6,8,13,15,18	2^{-12}
$(0,0,0,0,1,1,0,1,0,0,0,0,1,0,1,1) \xrightarrow{1r} (0,0,0,1,1,0,1,0,0,1,1,0,0,1,0,0)$	5,16,17	6,8,13,15,17	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,0,0,0,1,1,0,0) \xrightarrow{1r} (1,1,1,1,1,0,0,1,1,1,1,0,0,1,0,1)$	5,14,17,18	6,8,13,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,0,0,0,1,1,0,1) \xrightarrow{1r} (0,0,0,0,0,1,1,0,0,0,0,1,1,0,1,1)$	5,14,16	6,8,13	2^{-1}
$(0,0,0,0,1,1,0,1,0,0,0,0,1,1,1,0) \xrightarrow{1r} (0,0,1,1,1,0,0,0,1,1,1,0,0,1,0,1)$	5,14,17	6,8,13,15,17	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,0,0,0,1,1,1,1) \xrightarrow{1r} (1,1,0,0,0,1,1,1,0,0,0,1,1,0,1,1)$	5,14,16,18	6,8,13,15,18	2^{-1}
$(0,0,0,0,1,1,0,1,0,0,0,1,0,0,0,0) \xrightarrow{1r} (0,0,1,0,1,1,1,1,0,0,0,0,1,0,1)$	5,12,17	6,8,17	2^{-23}
$(0,0,0,0,1,1,0,1,0,0,0,1,0,0,0,1) \xrightarrow{1r} (1,1,0,1,0,0,0,0,0,1,1,1,1,0,1,1)$	5,12,16,18	6,8,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,0,0,1,0,0,1,0) \xrightarrow{1r} (1,1,1,0,1,1,1,0,1,0,0,0,0,1,0,1)$	5,12,17,18	6,8,15,17,18	2^{-23}
$(0,0,0,0,1,1,0,1,0,0,0,1,0,0,1,1) \xrightarrow{1r} (0,0,0,1,0,0,0,1,0,1,1,1,1,1,0,1)$	5,12,16	6,8,15	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,0,0,1,0,1,0,0) \xrightarrow{1r} (1,1,1,1,0,0,1,0,1,1,1,1,1,0,1,0)$	5,12,14,18	6,8,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,0,0,1,0,1,0,1) \xrightarrow{1r} (0,0,0,0,1,1,0,1,0,0,0,0,0,1,0,0)$	5,12,14,16,17	6,8,17	2^{-12}
$(0,0,0,0,1,1,0,1,0,0,0,1,0,1,1,0) \xrightarrow{1r} (0,0,1,1,0,0,1,1,1,1,1,1,1,0,1,0)$	5,12,14	6,8,15	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,0,0,1,0,1,1,1) \xrightarrow{1r} (1,1,0,0,1,1,0,0,0,0,0,0,0,1,0,0)$	5,12,14,16,17,18	6,8,15,17,18	2^{-12}
$(0,0,0,0,1,1,0,1,0,0,0,1,1,0,0,0) \xrightarrow{1r} (1,1,1,1,1,0,1,1,1,1,0,0,0,1,0,1)$	5,12,17,18	6,8,13,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,0,0,1,1,0,0,1) \xrightarrow{1r} (0,0,0,0,0,1,0,0,0,0,1,1,1,0,1,1)$	5,12,16	6,8,13	2^{-12}
$(0,0,0,0,1,1,0,1,0,0,0,1,1,0,1,0) \xrightarrow{1r} (0,0,1,1,1,0,1,0,1,1,0,0,0,1,0,1)$	5,12,17	6,8,13,15,17	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,0,0,1,1,0,1,1) \xrightarrow{1r} (1,1,0,0,0,1,0,1,0,0,1,1,1,0,1,1)$	5,12,16,18	6,8,13,15,18	2^{-12}
$(0,0,0,0,1,1,0,1,0,0,0,1,1,1,0,0) \xrightarrow{1r} (0,0,1,0,0,1,1,0,1,0,1,1,1,0,1,0)$	5,12,14	6,8,13	2^{-23}
$(0,0,0,0,1,1,0,1,0,0,0,1,1,1,0,1) \xrightarrow{1r} (1,1,0,1,1,0,0,1,0,1,0,0,0,1,0,0)$	5,12,14,16,17,18	6,8,13,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,0,0,1,1,1,1,0) \xrightarrow{1r} (1,1,1,0,0,1,1,1,1,0,1,1,1,0,1,0)$	5,12,14,18	6,8,13,15,18	2^{-23}
$(0,0,0,0,1,1,0,1,0,0,0,1,1,1,1,1) \xrightarrow{1r} (0,0,0,1,1,0,0,0,0,1,0,0,0,1,0,0)$	5,12,14,16,17	6,8,13,15,17	$2^{-17.5}$

Table 0.106 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,1,0,1,0,0,1,0,0,0,0,0) \xrightarrow{1r} (0,0,1,1,0,1,0,0,1,0,0,0,1,0,1,0)$	5	6,8,11	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,0,1,0,0,0,0,1) \xrightarrow{1r} (1,1,0,0,1,0,1,1,0,1,1,1,0,1,0,0)$	5,16,17,18	6,8,11,17,18	2^{-23}
$(0,0,0,0,1,1,0,1,0,0,1,0,0,0,1,0) \xrightarrow{1r} (1,1,1,1,0,1,0,1,1,0,0,0,1,0,1,0)$	5,18	6,8,11,15,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,0,1,0,0,0,1,1) \xrightarrow{1r} (0,0,0,0,1,0,1,0,0,1,1,1,0,1,0,0)$	5,16,17	6,8,11,15,17	2^{-23}
$(0,0,0,0,1,1,0,1,0,0,1,0,0,1,0,0) \xrightarrow{1r} (1,1,1,0,1,0,0,1,1,1,1,1,0,1,0,1)$	5,14,17,18	6,8,11,17,18	2^{-23}
$(0,0,0,0,1,1,0,1,0,0,1,0,0,1,0,1) \xrightarrow{1r} (0,0,0,1,0,1,1,0,0,0,0,0,1,0,1,1)$	5,14,16	6,8,11	$2^{-6.5}$
$(0,0,0,0,1,1,0,1,0,0,1,0,0,1,1,0) \xrightarrow{1r} (0,0,1,0,1,0,0,0,1,1,1,1,0,1,0,1)$	5,14,17	6,8,11,15,17	2^{-23}
$(0,0,0,0,1,1,0,1,0,0,1,0,0,1,1,1) \xrightarrow{1r} (1,1,0,1,0,1,1,1,0,0,0,0,1,0,1,1)$	5,14,16,18	6,8,11,15,18	$2^{-6.5}$
$(0,0,0,0,1,1,0,1,0,0,1,0,1,0,0,0) \xrightarrow{1r} (1,1,1,0,0,0,0,0,1,1,0,0,1,0,1,0)$	5,18	6,8,11,13,18	2^{-12}
$(0,0,0,0,1,1,0,1,0,0,1,0,1,0,0,1) \xrightarrow{1r} (0,0,0,1,1,1,1,0,0,1,1,0,1,0,0,0)$	5,16,17	6,8,11,13,17	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,0,1,0,1,0,1,0) \xrightarrow{1r} (0,0,1,0,0,0,0,1,1,1,0,0,1,0,1,0)$	5	6,8,11,13,15	2^{-12}
$(0,0,0,0,1,1,0,1,0,0,1,0,1,0,1,1) \xrightarrow{1r} (1,1,0,1,1,1,1,0,0,0,1,1,0,1,0,0)$	5,16,17,18	6,8,11,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,0,1,0,1,1,0,0) \xrightarrow{1r} (0,0,1,1,1,1,0,1,1,0,1,1,0,1,0,1)$	5,14,17	6,8,11,13,17	$2^{-28.5}$
$(0,0,0,0,1,1,0,1,0,0,1,0,1,1,0,1) \xrightarrow{1r} (1,1,0,0,0,0,1,0,0,1,0,0,1,0,1,1)$	5,14,16,18	6,8,11,13,18	2^{-12}
$(0,0,0,0,1,1,0,1,0,0,1,0,1,1,1,0) \xrightarrow{1r} (1,1,1,1,1,1,0,0,1,0,1,1,0,1,0,1)$	5,14,17,18	6,8,11,13,15,17,18	$2^{-28.5}$
$(0,0,0,0,1,1,0,1,0,0,1,0,1,1,1,1) \xrightarrow{1r} (0,0,0,0,0,0,1,1,0,1,0,0,1,0,1,1)$	5,14,16	6,8,11,13,15	2^{-12}
$(0,0,0,0,1,1,0,1,0,0,1,1,0,0,0,0) \xrightarrow{1r} (1,1,1,0,1,0,1,1,1,1,0,1,0,1,0,1)$	5,12,17,18	6,8,11,17,18	2^{-12}
$(0,0,0,0,1,1,0,1,0,0,1,1,0,0,0,1) \xrightarrow{1r} (0,0,0,1,0,1,0,0,0,0,1,0,1,0,1,1)$	5,12,16	6,8,11	$2^{-6.5}$
$(0,0,0,0,1,1,0,1,0,0,1,1,0,0,1,0) \xrightarrow{1r} (0,0,1,0,1,0,1,0,1,1,0,1,0,1,0,1)$	5,12,17	6,8,11,15,17	2^{-12}
$(0,0,0,0,1,1,0,1,0,0,1,1,0,0,1,1) \xrightarrow{1r} (1,1,0,1,0,1,0,1,0,0,1,0,1,0,1,1)$	5,12,16,18	6,8,11,15,18	$2^{-6.5}$
$(0,0,0,0,1,1,0,1,0,0,1,1,0,1,0,0) \xrightarrow{1r} (0,0,1,1,0,1,1,0,1,0,1,0,1,0,1,0)$	5,12,14	6,8,11	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,0,1,1,0,1,0,1) \xrightarrow{1r} (1,1,0,0,1,0,0,1,0,1,0,1,0,1,0,0)$	5,12,14,16,17,18	6,8,11,17,18	2^{-12}
$(0,0,0,0,1,1,0,1,0,0,1,1,0,1,1,0) \xrightarrow{1r} (1,1,1,1,0,1,1,1,1,0,1,0,1,0,1,0)$	5,12,14,18	6,8,11,15,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,0,1,1,0,1,1,1) \xrightarrow{1r} (0,0,0,0,1,0,0,0,0,0,1,0,1,0,1,0)$	5,12,14,16,17	6,8,11,15,17	2^{-12}
$(0,0,0,0,1,1,0,1,0,0,1,1,1,0,0,0) \xrightarrow{1r} (0,0,1,1,1,1,1,1,1,0,0,1,0,1,0,1)$	5,12,17	6,8,11,13,17	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,0,1,1,1,0,0,1) \xrightarrow{1r} (1,1,0,0,0,0,0,0,0,0,1,1,0,1,0,1)$	5,12,16,18	6,8,11,13,18	2^{-12}
$(0,0,0,0,1,1,0,1,0,0,1,1,1,0,1,0) \xrightarrow{1r} (1,1,1,1,1,1,1,0,1,0,0,1,0,1,0,1)$	5,12,17,18	6,8,11,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,0,1,1,1,0,1,1) \xrightarrow{1r} (0,0,0,0,0,0,0,1,0,1,1,0,1,0,1,1)$	5,12,16	6,8,11,13,15	2^{-12}
$(0,0,0,0,1,1,0,1,0,0,1,1,1,1,0,0) \xrightarrow{1r} (1,1,1,0,0,0,1,0,1,1,1,0,1,0,1,0)$	5,12,14,18	6,8,11,13,18	2^{-12}
$(0,0,0,0,1,1,0,1,0,0,1,1,1,1,0,1) \xrightarrow{1r} (0,0,0,1,1,1,0,1,0,0,0,1,0,1,0,0)$	5,12,14,16,17	6,8,11,13,17	$2^{-6.5}$
$(0,0,0,0,1,1,0,1,0,0,1,1,1,1,1,0) \xrightarrow{1r} (0,0,1,0,0,0,1,1,1,1,1,0,1,0,1,0)$	5,12,14	6,8,11,13,15	2^{-12}
$(0,0,0,0,1,1,0,1,0,0,1,1,1,1,1,1) \xrightarrow{1r} (1,1,0,1,1,1,0,0,0,0,0,1,0,1,0,0)$	5,12,14,16,17,18	6,8,11,13,15,17,18	$2^{-6.5}$

Table 0.107 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(2)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,1,0,1,0,1,0,0,0,0,0,0) \xrightarrow{1r} (0,0,0,0,0,1,0,1,1,0,0,0,1,1,0,1)$	5,10,17	6,8,17	2^{-23}
$(0,0,0,0,1,1,0,1,0,1,0,0,0,0,0,1) \xrightarrow{1r} (1,1,1,1,1,0,1,0,0,1,1,1,0,0,1,1)$	5,10,16,18	6,8,18	$2^{-28.5}$
$(0,0,0,0,1,1,0,1,0,1,0,0,0,0,1,0) \xrightarrow{1r} (1,1,0,0,0,1,0,0,1,0,0,0,1,1,0,1)$	5,10,17,18	6,8,15,17,18	2^{-23}
$(0,0,0,0,1,1,0,1,0,1,0,0,0,0,1,1) \xrightarrow{1r} (0,0,1,1,1,0,1,1,0,1,1,1,0,0,1,1)$	5,10,16	6,8,15	$2^{-28.5}$
$(0,0,0,0,1,1,0,1,0,1,0,0,0,1,0,0) \xrightarrow{1r} (1,1,0,1,1,0,0,0,1,1,1,1,0,0,1,0)$	5,10,14,18	6,8,18	$2^{-28.5}$
$(0,0,0,0,1,1,0,1,0,1,0,0,0,1,0,1) \xrightarrow{1r} (0,0,1,0,0,1,1,1,0,0,0,0,1,1,0,0)$	5,10,14,16,17	6,8,17	2^{-12}
$(0,0,0,0,1,1,0,1,0,1,0,0,0,1,1,0) \xrightarrow{1r} (0,0,0,1,1,0,0,1,1,1,1,1,0,0,1,0)$	5,10,14	6,8,15	$2^{-28.5}$
$(0,0,0,0,1,1,0,1,0,1,0,0,0,1,1,1) \xrightarrow{1r} (1,1,1,0,0,1,1,0,0,0,0,0,1,1,0,0)$	5,10,14,16,17,18	6,8,15,17,18	2^{-12}
$(0,0,0,0,1,1,0,1,0,1,0,0,1,0,0,0) \xrightarrow{1r} (1,1,0,1,0,0,0,1,1,1,0,0,1,1,0,1)$	5,10,17,18	6,8,13,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,1,0,0,1,0,0,1) \xrightarrow{1r} (0,0,1,0,1,1,1,0,0,0,1,1,0,0,1,1)$	5,10,16	6,8,13	2^{-23}
$(0,0,0,0,1,1,0,1,0,1,0,0,1,0,1,0) \xrightarrow{1r} (0,0,0,1,0,0,0,0,1,1,0,0,1,1,0,1)$	5,10,17	6,8,13,15,17	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,1,0,0,1,0,1,1) \xrightarrow{1r} (1,1,1,0,1,1,1,1,0,0,1,1,0,0,1,1)$	5,10,16,18	6,8,13,15,18	2^{-23}
$(0,0,0,0,1,1,0,1,0,1,0,0,1,1,0,0) \xrightarrow{1r} (0,0,0,0,1,1,0,0,1,0,1,1,0,0,1,0)$	5,10,14	6,8,13	2^{-34}
$(0,0,0,0,1,1,0,1,0,1,0,0,1,1,0,1) \xrightarrow{1r} (1,1,1,1,0,0,1,1,0,1,0,0,1,1,0,0)$	5,10,14,16,17,18	6,8,13,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,1,0,0,1,1,1,0) \xrightarrow{1r} (1,1,0,0,1,1,0,1,1,0,1,1,0,0,1,0)$	5,10,14,18	6,8,13,15,18	2^{-34}
$(0,0,0,0,1,1,0,1,0,1,0,0,1,1,1,1) \xrightarrow{1r} (0,0,1,1,0,0,1,0,0,1,0,0,1,1,0,0)$	5,10,14,16,17	6,8,13,15,17	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,1,0,1,0,0,0,0) \xrightarrow{1r} (1,1,0,1,1,0,1,0,1,1,0,1,0,0,1,0)$	5,10,12,18	6,8,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,1,0,1,0,0,0,1) \xrightarrow{1r} (0,0,1,0,0,1,0,1,0,0,1,0,1,1,0,0)$	5,10,12,16,17	6,8,17	2^{-12}
$(0,0,0,0,1,1,0,1,0,1,0,1,0,0,1,0) \xrightarrow{1r} (0,0,0,1,1,0,1,1,1,1,0,1,0,0,1,0)$	5,10,12	6,8,15	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,1,0,1,0,0,1,1) \xrightarrow{1r} (1,1,1,0,0,1,0,0,0,0,1,0,1,1,0,0)$	5,10,12,16,17,18	6,8,15,17,18	2^{-12}
$(0,0,0,0,1,1,0,1,0,1,0,1,0,1,0,0) \xrightarrow{1r} (0,0,0,0,0,1,1,1,1,0,1,0,1,1,0,1)$	5,10,12,14,17	6,8,17	2^{-23}
$(0,0,0,0,1,1,0,1,0,1,0,1,0,1,0,1) \xrightarrow{1r} (1,1,1,1,1,0,0,0,0,1,0,1,0,0,1,1)$	5,10,12,14,16,18	6,8,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,1,0,1,0,1,1,0) \xrightarrow{1r} (1,1,0,0,0,1,1,0,1,0,1,0,1,1,0,1)$	5,10,12,14,17,18	6,8,15,17,18	2^{-23}
$(0,0,0,0,1,1,0,1,0,1,0,1,0,1,1,1) \xrightarrow{1r} (0,0,1,1,1,0,0,1,0,1,0,1,0,0,1,1)$	5,10,12,14,16	6,8,15	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,1,0,1,0,1,0,0) \xrightarrow{1r} (0,0,0,0,1,1,1,0,1,0,0,1,0,0,1,0)$	5,10,12	6,8,13	2^{-23}
$(0,0,0,0,1,1,0,1,0,1,0,1,1,0,0,1) \xrightarrow{1r} (1,1,1,1,0,0,0,1,0,1,1,0,1,1,0,0)$	5,10,12,16,17,18	6,8,13,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,1,0,1,1,0,1,0) \xrightarrow{1r} (1,1,0,0,1,1,1,1,1,0,0,1,0,0,1,0)$	5,10,12,18	6,8,13,15,18	2^{-23}
$(0,0,0,0,1,1,0,1,0,1,0,1,1,0,1,1) \xrightarrow{1r} (0,0,1,1,0,0,0,0,0,1,1,0,1,1,0,0)$	5,10,12,16,17	6,8,13,15,17	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,1,0,1,1,1,0,0) \xrightarrow{1r} (1,1,0,1,0,0,1,1,1,1,1,0,1,1,0,1)$	5,10,12,14,17,18	6,8,13,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,1,0,1,1,1,0,1) \xrightarrow{1r} (0,0,1,0,1,1,0,0,0,0,0,1,0,0,1,1)$	5,10,12,14,16	6,8,13	2^{-12}
$(0,0,0,0,1,1,0,1,0,1,0,1,1,1,1,0) \xrightarrow{1r} (0,0,0,1,0,0,1,0,1,1,1,0,1,1,0,1)$	5,10,12,14,17	6,8,13,15,17	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,1,0,1,1,1,1,1) \xrightarrow{1r} (1,1,1,0,1,1,0,1,0,0,0,1,0,0,1,1)$	5,10,12,14,16,18	6,8,13,15,18	2^{-12}

Table 0.108 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,1,0,1,0,1,1,0,0,0,0,0) \xrightarrow{1r} (1,1,0,0,0,0,0,1,1,1,0,1,1,1,0,1)$	5,10,17,18	6,8,11,17,18	2^{-12}
$(0,0,0,0,1,1,0,1,0,1,1,0,0,0,0,1) \xrightarrow{1r} (0,0,1,1,1,1,1,0,0,0,1,0,0,0,1,1)$	5,10,16	6,8,11	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,1,1,0,0,0,1,0) \xrightarrow{1r} (0,0,0,0,0,0,0,0,1,1,0,1,1,1,0,1)$	5,10,17	6,8,11,15,17	2^{-12}
$(0,0,0,0,1,1,0,1,0,1,1,0,0,0,1,1) \xrightarrow{1r} (1,1,1,1,1,1,1,1,0,0,1,0,0,0,1,1)$	5,10,16,18	6,8,11,15,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,1,1,0,0,1,0,0) \xrightarrow{1r} (0,0,0,1,1,1,0,0,1,0,1,0,0,0,1,0)$	5,10,14	6,8,11	$2^{-28.5}$
$(0,0,0,0,1,1,0,1,0,1,1,0,0,1,0,1) \xrightarrow{1r} (1,1,1,0,0,0,1,1,0,1,0,1,1,1,0,0)$	5,10,14,16,17,18	6,8,11,17,18	2^{-12}
$(0,0,0,0,1,1,0,1,0,1,1,0,0,1,1,0) \xrightarrow{1r} (1,1,0,1,1,1,0,1,1,0,1,0,0,0,1,0)$	5,10,14,18	6,8,11,15,18	$2^{-28.5}$
$(0,0,0,0,1,1,0,1,0,1,1,0,0,1,1,1) \xrightarrow{1r} (0,0,1,0,0,0,1,0,0,1,0,1,1,1,0,0)$	5,10,14,16,17	6,8,11,15,17	2^{-12}
$(0,0,0,0,1,1,0,1,0,1,1,0,1,0,0,0) \xrightarrow{1r} (0,0,0,1,0,1,0,1,1,0,0,1,1,1,0,1)$	5,10,17	6,8,11,13,17	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,1,1,0,1,0,0,1) \xrightarrow{1r} (1,1,1,0,1,0,1,0,0,1,1,0,0,0,1,1)$	5,10,16,18	6,8,11,13,18	2^{-23}
$(0,0,0,0,1,1,0,1,0,1,1,0,1,0,1,0) \xrightarrow{1r} (1,1,0,1,0,1,0,0,1,0,0,1,1,1,0,1)$	5,10,17,18	6,8,11,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,1,1,0,1,0,1,1) \xrightarrow{1r} (0,0,1,0,1,0,1,1,0,1,1,0,0,0,1,1)$	5,10,16	6,8,11,13,15	2^{-23}
$(0,0,0,0,1,1,0,1,0,1,1,0,1,1,0,0) \xrightarrow{1r} (1,1,0,0,1,0,0,0,1,1,1,0,0,0,1,0)$	5,10,14,18	6,8,11,13,18	2^{-23}
$(0,0,0,0,1,1,0,1,0,1,1,0,1,1,0,1) \xrightarrow{1r} (0,0,1,1,0,1,1,1,0,0,0,1,1,1,0,0)$	5,10,14,16,17	6,8,11,13,17	$2^{-6.5}$
$(0,0,0,0,1,1,0,1,0,1,1,0,1,1,1,0) \xrightarrow{1r} (0,0,0,0,1,0,0,1,1,1,1,0,0,0,1,0)$	5,10,14	6,8,11,13,15	2^{-23}
$(0,0,0,0,1,1,0,1,0,1,1,0,1,1,1,1) \xrightarrow{1r} (1,1,1,1,0,1,1,0,0,0,0,1,1,1,0,0)$	5,10,14,16,17,18	6,8,11,13,15,17,18	$2^{-6.5}$
$(0,0,0,0,1,1,0,1,0,1,1,1,0,0,0,0) \xrightarrow{1r} (0,0,0,1,1,1,1,0,1,0,0,0,0,0,1,0)$	5,10,12	6,8,11	$2^{-28.5}$
$(0,0,0,0,1,1,0,1,0,1,1,1,0,0,0,1) \xrightarrow{1r} (1,1,1,0,0,0,0,1,0,1,1,1,1,1,0,0)$	5,10,12,16,17,18	6,8,11,17,18	2^{-23}
$(0,0,0,0,1,1,0,1,0,1,1,1,0,0,1,0) \xrightarrow{1r} (1,1,0,1,1,1,1,1,1,0,0,0,0,0,1,0)$	5,10,12,18	6,8,11,15,18	$2^{-28.5}$
$(0,0,0,0,1,1,0,1,0,1,1,1,0,0,1,1) \xrightarrow{1r} (0,0,1,0,0,0,0,0,0,1,1,1,1,1,0,0)$	5,10,12,16,17	6,8,11,15,17	2^{-23}
$(0,0,0,0,1,1,0,1,0,1,1,1,0,1,0,0) \xrightarrow{1r} (1,1,0,0,0,0,1,1,1,1,1,1,1,0,1)$	5,10,12,14,17,18	6,8,11,17,18	2^{-23}
$(0,0,0,0,1,1,0,1,0,1,1,1,0,1,0,1) \xrightarrow{1r} (0,0,1,1,1,1,0,0,0,0,0,0,0,0,1,1)$	5,10,12,14,16	6,8,11	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,1,1,1,0,1,1,0) \xrightarrow{1r} (0,0,0,0,0,0,1,0,1,1,1,1,1,1,0,1)$	5,10,12,14,17	6,8,11,15,17	2^{-23}
$(0,0,0,0,1,1,0,1,0,1,1,1,0,1,1,1) \xrightarrow{1r} (1,1,1,1,1,1,0,1,0,0,0,0,0,0,1,1)$	5,10,12,14,16,18	6,8,11,15,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,1,1,1,1,0,0,0) \xrightarrow{1r} (1,1,0,0,1,0,1,0,1,1,0,0,0,0,1,0)$	5,10,12,18	6,8,11,13,18	2^{-23}
$(0,0,0,0,1,1,0,1,0,1,1,1,1,0,0,1) \xrightarrow{1r} (0,0,1,1,0,1,0,1,0,0,1,1,1,1,0,0)$	5,10,12,16,17	6,8,11,13,17	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,1,1,1,1,0,1,0) \xrightarrow{1r} (0,0,0,0,1,0,1,1,1,1,0,0,0,0,1,0)$	5,10,12	6,8,11,13,15	2^{-23}
$(0,0,0,0,1,1,0,1,0,1,1,1,1,0,1,1) \xrightarrow{1r} (1,1,1,1,0,1,0,0,0,0,1,1,1,1,0,0)$	5,10,12,16,17,18	6,8,11,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,0,1,1,1,1,1,0,0) \xrightarrow{1r} (0,0,0,1,0,1,1,1,1,0,1,1,1,1,0,1)$	5,10,12,14,17	6,8,11,13,17	$2^{-28.5}$
$(0,0,0,0,1,1,0,1,0,1,1,1,1,1,0,1) \xrightarrow{1r} (1,1,1,0,1,0,0,0,0,1,0,0,0,0,1,1)$	5,10,12,14,16,18	6,8,11,13,18	2^{-23}
$(0,0,0,0,1,1,0,1,0,1,1,1,1,1,1,0) \xrightarrow{1r} (1,1,0,1,0,1,1,0,1,0,1,1,1,1,0,1)$	5,10,12,14,17,18	6,8,11,13,15,17,18	$2^{-28.5}$
$(0,0,0,0,1,1,0,1,0,1,1,1,1,1,1,1) \xrightarrow{1r} (0,0,1,0,1,0,0,1,0,1,0,0,0,0,1,1)$	5,10,12,14,16	6,8,11,13,15	2^{-23}

Table 0.109 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,1,0,1,1,0,0,0,0,0,0,0) \xrightarrow{1r} (0,1,1,0,0,1,0,1,1,0,0,0,1,1,1,0)$	5	6,8,9	2^{-23}
$(0,0,0,0,1,1,0,1,1,0,0,0,0,0,0,1) \xrightarrow{1r} (1,0,0,1,1,0,1,0,0,1,1,1,0,0,0,0)$	5,16,17,18	6,8,9,17,18	$2^{-28.5}$
$(0,0,0,0,1,1,0,1,1,0,0,0,0,0,1,0) \xrightarrow{1r} (1,0,1,0,0,1,0,0,1,0,0,0,1,1,1,0)$	5,18	6,8,9,15,18	2^{-23}
$(0,0,0,0,1,1,0,1,1,0,0,0,0,0,1,1) \xrightarrow{1r} (0,1,0,1,1,0,1,1,0,1,1,1,0,0,0,0)$	5,16,17	6,8,9,15,17	$2^{-28.5}$
$(0,0,0,0,1,1,0,1,1,0,0,0,0,1,0,0) \xrightarrow{1r} (1,0,1,1,1,0,0,0,1,1,1,1,0,0,0,1)$	5,14,17,18	6,8,9,17,18	$2^{-28.5}$
$(0,0,0,0,1,1,0,1,1,0,0,0,0,1,0,1) \xrightarrow{1r} (0,1,0,0,0,1,1,1,0,0,0,0,1,1,1,1)$	5,14,16	6,8,9	2^{-12}
$(0,0,0,0,1,1,0,1,1,0,0,0,0,1,1,0) \xrightarrow{1r} (0,1,1,1,1,0,0,1,1,1,1,1,0,0,0,1)$	5,14,17	6,8,9,15,17	$2^{-28.5}$
$(0,0,0,0,1,1,0,1,1,0,0,0,0,1,1,1) \xrightarrow{1r} (1,0,0,0,0,1,1,0,0,0,0,0,1,1,1,1)$	5,14,16,18	6,8,9,15,18	2^{-12}
$(0,0,0,0,1,1,0,1,1,0,0,0,1,0,0,0) \xrightarrow{1r} (1,0,1,1,0,0,0,1,1,1,0,0,1,1,1,0)$	5,18	6,8,9,13,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,0,0,0,1,0,0,1) \xrightarrow{1r} (0,1,0,0,1,1,1,0,0,0,1,1,0,0,0,0)$	5,16,17	6,8,9,13,17	2^{-23}
$(0,0,0,0,1,1,0,1,1,0,0,0,1,0,1,0) \xrightarrow{1r} (0,1,1,1,0,0,0,0,1,1,0,0,1,1,1,0)$	5	6,8,9,13,15	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,0,0,0,1,0,1,1) \xrightarrow{1r} (1,0,0,0,1,1,1,1,0,0,1,1,0,0,0,0)$	5,16,17,18	6,8,9,13,15,17,18	2^{-23}
$(0,0,0,0,1,1,0,1,1,0,0,0,1,1,0,0) \xrightarrow{1r} (0,1,1,0,1,1,0,0,1,0,1,1,0,0,0,1)$	5,14,17	6,8,9,13,17	2^{-34}
$(0,0,0,0,1,1,0,1,1,0,0,0,1,1,0,1) \xrightarrow{1r} (1,0,0,1,0,0,1,1,0,1,0,0,1,1,1,1)$	5,14,16,18	6,8,9,13,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,0,0,0,1,1,1,0) \xrightarrow{1r} (1,0,1,0,1,1,0,1,1,0,1,1,0,0,0,1)$	5,14,17,18	6,8,9,13,15,17,18	2^{-34}
$(0,0,0,0,1,1,0,1,1,0,0,0,1,1,1,1) \xrightarrow{1r} (0,1,0,1,0,0,1,0,0,1,0,0,1,1,1,1)$	5,14,16	6,8,9,13,15	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,0,0,1,0,0,0,0) \xrightarrow{1r} (1,0,1,1,1,0,1,0,1,1,0,1,0,0,0,1)$	5,12,17,18	6,8,9,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,0,0,1,0,0,0,1) \xrightarrow{1r} (0,1,0,0,0,1,0,1,0,0,1,0,1,1,1,1)$	5,12,16	6,8,9	2^{-12}
$(0,0,0,0,1,1,0,1,1,0,0,1,0,0,1,0) \xrightarrow{1r} (0,1,1,1,1,0,1,1,1,1,0,1,0,0,0,1)$	5,12,17	6,8,9,15,17	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,0,0,1,0,0,1,1) \xrightarrow{1r} (1,0,0,0,0,1,0,0,0,0,1,0,1,1,1,1)$	5,12,16,18	6,8,9,15,18	2^{-12}
$(0,0,0,0,1,1,0,1,1,0,0,1,0,1,0,0) \xrightarrow{1r} (0,1,1,0,0,1,1,1,1,0,1,0,1,1,1,0)$	5,12,14	6,8,9	2^{-23}
$(0,0,0,0,1,1,0,1,1,0,0,1,0,1,0,1) \xrightarrow{1r} (1,0,0,1,1,0,0,0,0,1,0,1,0,0,0,0)$	5,12,14,16,17,18	6,8,9,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,0,0,1,0,1,1,0) \xrightarrow{1r} (1,0,1,0,0,1,1,0,1,0,1,0,1,1,1,0)$	5,12,14,18	6,8,9,15,18	2^{-23}
$(0,0,0,0,1,1,0,1,1,0,0,1,0,1,1,1) \xrightarrow{1r} (0,1,0,1,1,0,0,1,0,1,0,1,0,0,0,0)$	5,12,14,16,17	6,8,9,15,17	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,0,0,1,1,0,0,0) \xrightarrow{1r} (0,1,1,0,1,1,1,0,1,0,1,0,0,0,0,1)$	5,12,17	6,8,9,13,17	2^{-23}
$(0,0,0,0,1,1,0,1,1,0,0,1,1,0,0,1) \xrightarrow{1r} (1,0,0,1,0,0,0,1,0,1,1,0,1,1,1,1)$	5,12,16,18	6,8,9,13,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,0,0,1,1,0,1,0) \xrightarrow{1r} (1,0,1,0,1,1,1,1,1,0,0,1,0,0,0,1)$	5,12,17,18	6,8,9,13,15,17,18	2^{-23}
$(0,0,0,0,1,1,0,1,1,0,0,1,1,0,1,1) \xrightarrow{1r} (0,1,0,1,0,0,0,0,0,1,1,0,1,1,1,1)$	5,12,16	6,8,9,13,15	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,0,0,1,1,1,0,0) \xrightarrow{1r} (1,0,1,1,0,0,1,1,1,1,1,0,1,1,1,0)$	5,12,14,18	6,8,9,13,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,0,0,1,1,1,0,1) \xrightarrow{1r} (0,1,0,0,1,1,0,0,0,0,0,1,0,0,0,0)$	5,12,14,16,17	6,8,9,13,17	2^{-12}
$(0,0,0,0,1,1,0,1,1,0,0,1,1,1,1,0) \xrightarrow{1r} (0,1,1,1,0,0,1,0,1,1,1,0,1,1,1,0)$	5,12,14	6,8,9,13,15	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,0,0,1,1,1,1,1) \xrightarrow{1r} (1,0,0,0,1,1,0,1,0,0,0,1,0,0,0,0)$	5,12,14,16,17,18	6,8,9,13,15,17,18	2^{-12}

Table 0.110 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,1,0,1,1,0,1,0,0,0,0,0) \xrightarrow{1r} (1,0,1,0,0,0,0,1,1,1,0,1,1,1,1,0)$	5,18	6,8,9,11,18	2^{-12}
$(0,0,0,0,1,1,0,1,1,0,1,0,0,0,0,1) \xrightarrow{1r} (0,1,0,1,1,1,1,0,0,0,1,0,0,0,0,0)$	5,16,17	6,8,9,11,17	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,0,1,0,0,0,1,0) \xrightarrow{1r} (0,1,1,0,0,0,0,0,1,1,0,1,1,1,1,0)$	5	6,8,9,11,15	2^{-12}
$(0,0,0,0,1,1,0,1,1,0,1,0,0,0,1,1) \xrightarrow{1r} (1,0,0,1,1,1,1,1,0,0,1,0,0,0,0,0)$	5,16,17,18	6,8,9,11,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,0,1,0,0,1,0,0) \xrightarrow{1r} (0,1,1,1,1,1,0,0,1,0,1,0,0,0,0,1)$	5,14,17	6,8,9,11,17	$2^{-28.5}$
$(0,0,0,0,1,1,0,1,1,0,1,0,0,1,0,1) \xrightarrow{1r} (1,0,0,0,0,0,1,1,0,1,0,1,1,1,1,1)$	5,14,16,18	6,8,9,11,18	2^{-12}
$(0,0,0,0,1,1,0,1,1,0,1,0,0,1,1,0) \xrightarrow{1r} (1,0,1,1,1,1,0,1,1,0,1,0,0,0,0,1)$	5,14,17,18	6,8,9,11,15,17,18	$2^{-28.5}$
$(0,0,0,0,1,1,0,1,1,0,1,0,0,1,1,1) \xrightarrow{1r} (0,1,0,0,0,0,1,0,0,1,0,1,1,1,1,1)$	5,14,16	6,8,9,11,15	2^{-12}
$(0,0,0,0,1,1,0,1,1,0,1,0,1,0,0,0) \xrightarrow{1r} (0,1,1,1,0,1,0,1,1,0,0,1,1,1,1,0)$	5	6,8,9,11,13	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,0,1,0,1,0,0,1) \xrightarrow{1r} (1,0,0,0,1,0,1,0,0,1,1,0,0,0,0,0)$	5,16,17,18	6,8,9,11,13,17,18	2^{-23}
$(0,0,0,0,1,1,0,1,1,0,1,0,1,0,1,0) \xrightarrow{1r} (1,0,1,1,0,1,0,0,1,0,0,1,1,1,1,0)$	5,18	6,8,9,11,13,15,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,0,1,0,1,0,1,1) \xrightarrow{1r} (0,1,0,0,1,0,1,1,0,1,1,0,0,0,0,0)$	5,16,17	6,8,9,11,13,15,17	2^{-23}
$(0,0,0,0,1,1,0,1,1,0,1,0,1,1,0,0) \xrightarrow{1r} (1,0,1,0,1,0,0,0,1,1,1,0,0,0,0,1)$	5,14,17,18	6,8,9,11,13,17,18	2^{-23}
$(0,0,0,0,1,1,0,1,1,0,1,0,1,1,0,1) \xrightarrow{1r} (0,1,0,1,0,1,1,1,0,0,0,1,1,1,1,1)$	5,14,16	6,8,9,11,13	$2^{-6.5}$
$(0,0,0,0,1,1,0,1,1,0,1,0,1,1,1,0) \xrightarrow{1r} (0,1,1,0,1,0,0,1,1,1,1,0,0,0,0,1)$	5,14,17	6,8,9,11,13,15,17	2^{-23}
$(0,0,0,0,1,1,0,1,1,0,1,0,1,1,1,1) \xrightarrow{1r} (1,0,0,1,0,1,1,0,0,0,0,1,1,1,1,1)$	5,14,16,18	6,8,9,11,13,15,18	$2^{-6.5}$
$(0,0,0,0,1,1,0,1,1,0,1,1,0,0,0,0) \xrightarrow{1r} (0,1,1,1,1,1,1,0,1,0,0,0,0,0,0,1)$	5,12,17	6,8,9,11,17	$2^{-28.5}$
$(0,0,0,0,1,1,0,1,1,0,1,1,0,0,0,1) \xrightarrow{1r} (1,0,0,0,0,0,0,1,0,1,1,1,1,1,1,1)$	5,12,16,18	6,8,9,11,18	2^{-23}
$(0,0,0,0,1,1,0,1,1,0,1,1,0,0,1,0) \xrightarrow{1r} (1,0,1,1,1,1,1,1,1,0,0,0,0,0,0,1)$	5,12,17,18	6,8,9,11,15,17,18	$2^{-28.5}$
$(0,0,0,0,1,1,0,1,1,0,1,1,0,0,1,1) \xrightarrow{1r} (0,1,0,0,0,0,0,0,0,1,1,1,1,1,1,1)$	5,12,16	6,8,9,11,15	2^{-23}
$(0,0,0,0,1,1,0,1,1,0,1,1,0,1,0,0) \xrightarrow{1r} (1,0,1,0,0,0,1,1,1,1,1,1,1,1,1,0)$	5,12,14,18	6,8,9,11,18	2^{-23}
$(0,0,0,0,1,1,0,1,1,0,1,1,0,1,0,1) \xrightarrow{1r} (0,1,0,1,1,1,0,0,0,0,0,0,0,0,0,0)$	5,12,14,16,17	6,8,9,11,17	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,0,1,1,0,1,1,0) \xrightarrow{1r} (0,1,1,0,0,0,1,0,1,1,1,1,1,1,1,0)$	5,12,14	6,8,9,11,15	2^{-23}
$(0,0,0,0,1,1,0,1,1,0,1,1,0,1,1,1) \xrightarrow{1r} (1,0,0,1,1,1,0,1,0,0,0,0,0,0,0,0)$	5,12,14,16,17,18	6,8,9,11,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,0,1,1,1,0,0,0) \xrightarrow{1r} (1,0,1,0,1,0,1,0,1,1,1,0,0,0,0,1)$	5,12,17,18	6,8,9,11,13,17,18	2^{-23}
$(0,0,0,0,1,1,0,1,1,0,1,1,1,0,0,1) \xrightarrow{1r} (0,1,0,1,0,1,0,1,0,0,1,1,1,1,1,1)$	5,12,16	6,8,9,11,13	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,0,1,1,1,0,1,0) \xrightarrow{1r} (0,1,1,0,1,0,1,1,1,1,0,0,0,0,0,1)$	5,12,17	6,8,9,11,13,15,17	2^{-23}
$(0,0,0,0,1,1,0,1,1,0,1,1,1,0,1,1) \xrightarrow{1r} (1,0,0,1,0,1,0,0,0,0,1,1,1,1,1,1)$	5,12,16,18	6,8,9,11,13,15,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,0,1,1,1,1,0,0) \xrightarrow{1r} (0,1,1,1,0,1,1,1,1,0,1,1,1,1,1,0)$	5,12,14	6,8,9,11,13	$2^{-28.5}$
$(0,0,0,0,1,1,0,1,1,0,1,1,1,1,0,1) \xrightarrow{1r} (1,0,0,0,1,0,0,0,0,1,0,0,0,0,0,0)$	5,12,14,16,17,18	6,8,9,11,13,17,18	2^{-23}
$(0,0,0,0,1,1,0,1,1,0,1,1,1,1,1,0) \xrightarrow{1r} (1,0,1,1,0,1,1,0,1,0,1,1,1,1,1,0)$	5,12,14,18	6,8,9,11,13,15,18	$2^{-28.5}$
$(0,0,0,0,1,1,0,1,1,0,1,1,1,1,1,1) \xrightarrow{1r} (0,1,0,0,1,0,0,1,0,1,0,1,0,0,0,0)$	5,12,14,16,17	6,8,9,11,13,15,17	2^{-23}

Table 0.111 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,1,0,1,1,1,0,0,0,0,0,0) \xrightarrow{1r} (1,0,0,1,0,0,0,0,1,1,0,1,1,0,0,1)$	5,10,17,18	6,8,9,17,18	$2^{-6.5}$
$(0,0,0,0,1,1,0,1,1,1,0,0,0,0,0,1) \xrightarrow{1r} (0,1,1,0,1,1,1,1,0,0,1,0,0,1,1,1)$	5,10,16	6,8,9	2^{-12}
$(0,0,0,0,1,1,0,1,1,1,0,0,0,0,1,0) \xrightarrow{1r} (0,1,0,1,0,0,0,1,1,1,0,1,1,0,0,1)$	5,10,17	6,8,9,15,17	$2^{-6.5}$
$(0,0,0,0,1,1,0,1,1,1,0,0,0,0,1,1) \xrightarrow{1r} (1,0,1,0,1,1,1,0,0,0,1,0,0,1,1,1)$	5,10,16,18	6,8,9,15,18	2^{-12}
$(0,0,0,0,1,1,0,1,1,1,0,0,0,1,0,0) \xrightarrow{1r} (0,1,0,0,1,1,0,1,1,0,1,0,0,1,1,0)$	5,10,14	6,8,9	2^{-23}
$(0,0,0,0,1,1,0,1,1,1,0,0,0,1,0,1) \xrightarrow{1r} (1,0,1,1,0,0,1,0,0,1,0,1,1,0,0,0)$	5,10,14,16,17,18	6,8,9,17,18	$2^{-6.5}$
$(0,0,0,0,1,1,0,1,1,1,0,0,0,1,1,0) \xrightarrow{1r} (1,0,0,0,1,1,0,0,1,0,1,0,0,1,1,0)$	5,10,14,18	6,8,9,15,18	2^{-23}
$(0,0,0,0,1,1,0,1,1,1,0,0,0,1,1,1) \xrightarrow{1r} (0,1,1,1,0,0,1,1,0,1,0,1,1,0,0,0)$	5,10,14,16,17	6,8,9,15,17	$2^{-6.5}$
$(0,0,0,0,1,1,0,1,1,1,0,0,1,0,0,0) \xrightarrow{1r} (0,1,0,0,0,1,0,0,1,0,0,1,1,0,0,1)$	5,10,17	6,8,9,13,17	2^{-12}
$(0,0,0,0,1,1,0,1,1,1,0,0,1,0,0,1) \xrightarrow{1r} (1,0,1,1,1,0,1,1,0,1,1,0,0,1,1,1)$	5,10,16,18	6,8,9,13,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,1,0,0,1,0,1,0) \xrightarrow{1r} (1,0,0,0,0,1,0,1,1,0,0,1,1,0,0,1)$	5,10,17,18	6,8,9,13,15,17,18	2^{-12}
$(0,0,0,0,1,1,0,1,1,1,0,0,1,0,1,1) \xrightarrow{1r} (0,1,1,1,1,0,1,0,0,1,1,0,0,1,1,1)$	5,10,16	6,8,9,13,15	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,1,0,0,1,1,0,0) \xrightarrow{1r} (1,0,0,1,1,0,0,1,1,1,1,0,0,1,1,0)$	5,10,14,18	6,8,9,13,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,1,0,0,1,1,0,1) \xrightarrow{1r} (0,1,1,0,0,1,1,0,0,0,0,1,1,0,0,0)$	5,10,14,16,17	6,8,9,13,17	2^{-1}
$(0,0,0,0,1,1,0,1,1,1,0,0,1,1,1,0) \xrightarrow{1r} (0,1,0,1,1,0,0,0,1,1,1,0,0,1,1,0)$	5,10,14	6,8,9,13,15	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,1,0,0,1,1,1,1) \xrightarrow{1r} (1,0,1,0,0,1,1,1,0,0,0,1,1,0,0,0)$	5,10,14,16,17,18	6,8,9,13,15,17,18	2^{-1}
$(0,0,0,0,1,1,0,1,1,1,0,1,0,0,0,0) \xrightarrow{1r} (0,1,0,0,1,1,1,1,0,0,0,0,1,1,0)$	5,10,12	6,8,9	2^{-23}
$(0,0,0,0,1,1,0,1,1,1,0,1,0,0,0,1) \xrightarrow{1r} (1,0,1,1,0,0,0,0,0,1,1,1,1,0,0,0)$	5,10,12,16,17,18	6,8,9,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,1,0,1,0,0,1,0) \xrightarrow{1r} (1,0,0,0,1,1,1,0,1,0,0,0,0,1,1,0)$	5,10,12,18	6,8,9,15,18	2^{-23}
$(0,0,0,0,1,1,0,1,1,1,0,1,0,0,1,1) \xrightarrow{1r} (0,1,1,1,0,0,0,1,0,1,1,1,1,0,0,0)$	5,10,12,16,17	6,8,9,15,17	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,1,0,1,0,1,0,0) \xrightarrow{1r} (1,0,0,1,0,0,1,0,1,1,1,1,1,0,0,1)$	5,10,12,14,17,18	6,8,9,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,1,0,1,0,1,0,1) \xrightarrow{1r} (0,1,1,0,1,1,0,1,0,0,0,0,0,1,1,1)$	5,10,12,14,16	6,8,9	2^{-12}
$(0,0,0,0,1,1,0,1,1,1,0,1,0,1,1,0) \xrightarrow{1r} (0,1,0,1,0,0,1,1,1,1,1,1,1,0,0,1)$	5,10,12,14,17	6,8,9,15,17	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,1,0,1,0,1,1,1) \xrightarrow{1r} (1,0,1,0,1,1,0,0,0,0,0,0,0,1,1,1)$	5,10,12,14,16,18	6,8,9,15,18	2^{-12}
$(0,0,0,0,1,1,0,1,1,1,0,1,1,0,0,0) \xrightarrow{1r} (1,0,0,1,1,0,1,1,1,1,0,0,0,1,1,0)$	5,10,12,18	6,8,9,13,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,1,0,1,1,0,0,1) \xrightarrow{1r} (0,1,1,0,0,1,0,0,0,0,1,1,1,0,0,0)$	5,10,12,16,17	6,8,9,13,17	2^{-12}
$(0,0,0,0,1,1,0,1,1,1,0,1,1,0,1,0) \xrightarrow{1r} (0,1,0,1,1,0,1,0,1,1,0,0,0,1,1,0)$	5,10,12	6,8,9,13,15	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,1,0,1,1,0,1,1) \xrightarrow{1r} (1,0,1,0,0,1,0,1,0,0,1,1,1,0,0,0)$	5,10,12,16,17,18	6,8,9,13,15,17,18	2^{-12}
$(0,0,0,0,1,1,0,1,1,1,0,1,1,1,0,0) \xrightarrow{1r} (0,1,0,0,0,1,1,0,1,0,1,1,1,0,0,1)$	5,10,12,14,17	6,8,9,13,17	2^{-23}
$(0,0,0,0,1,1,0,1,1,1,0,1,1,1,0,1) \xrightarrow{1r} (1,0,1,1,1,0,0,1,0,1,0,0,0,1,1,1)$	5,10,12,14,16,18	6,8,9,13,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,1,0,1,1,1,1,0) \xrightarrow{1r} (1,0,0,0,0,1,1,1,1,0,1,1,1,0,0,1)$	5,10,12,14,17,18	6,8,9,13,15,17,18	2^{-23}
$(0,0,0,0,1,1,0,1,1,1,0,1,1,1,1,1) \xrightarrow{1r} (0,1,1,1,1,0,0,0,0,1,0,0,0,1,1,1)$	5,10,12,14,16	6,8,9,13,15	$2^{-17.5}$

Table 0.112 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,1,0,1,1,1,1,0,0,0,0,0) \xrightarrow{1r} (0,1,0,1,0,1,0,0,1,0,0,0,1,0,0,1)$	5,10,17	6,8,9,11,17	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,1,1,0,0,0,0,1) \xrightarrow{1r} (1,0,1,0,1,0,1,1,0,1,1,1,0,1,1,1)$	5,10,16,18	6,8,9,11,18	2^{-23}
$(0,0,0,0,1,1,0,1,1,1,1,0,0,0,1,0) \xrightarrow{1r} (1,0,0,1,0,1,0,1,1,0,0,0,1,0,0,1)$	5,10,17,18	6,8,9,11,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,1,1,0,0,0,1,1) \xrightarrow{1r} (0,1,1,0,1,0,1,0,0,1,1,1,0,1,1,1)$	5,10,16	6,8,9,11,15	2^{-23}
$(0,0,0,0,1,1,0,1,1,1,1,0,0,1,0,0) \xrightarrow{1r} (1,0,0,0,1,0,0,1,1,1,1,1,0,1,1,0)$	5,10,14,18	6,8,9,11,18	2^{-23}
$(0,0,0,0,1,1,0,1,1,1,1,0,0,1,0,1) \xrightarrow{1r} (0,1,1,1,0,1,1,0,0,0,0,0,1,0,0,0)$	5,10,14,16,17	6,8,9,11,17	$2^{-6.5}$
$(0,0,0,0,1,1,0,1,1,1,1,0,0,1,1,0) \xrightarrow{1r} (0,1,0,0,1,0,0,0,1,1,1,1,0,1,1,0)$	5,10,14	6,8,9,11,15	2^{-23}
$(0,0,0,0,1,1,0,1,1,1,1,0,0,1,1,1) \xrightarrow{1r} (1,0,1,1,0,1,1,1,0,0,0,0,1,0,0,0)$	5,10,14,16,17,18	6,8,9,11,15,17,18	$2^{-6.5}$
$(0,0,0,0,1,1,0,1,1,1,1,0,1,0,0,0) \xrightarrow{1r} (1,0,0,0,0,0,0,0,1,1,0,0,1,0,0,1)$	5,10,17,18	6,8,9,11,13,17,18	2^{-12}
$(0,0,0,0,1,1,0,1,1,1,1,0,1,0,0,1) \xrightarrow{1r} (0,1,1,1,1,1,1,1,0,0,1,1,0,1,1,1)$	5,10,16	6,8,9,11,13	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,1,1,0,1,0,1,0) \xrightarrow{1r} (0,1,0,0,0,0,0,0,1,1,1,0,0,1,0,0,1)$	5,10,17	6,8,9,11,13,15,17	2^{-12}
$(0,0,0,0,1,1,0,1,1,1,1,0,1,0,1,1) \xrightarrow{1r} (1,0,1,1,1,1,1,0,0,0,1,1,0,1,1,1)$	5,10,16,18	6,8,9,11,13,15,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,1,1,0,1,1,0,0) \xrightarrow{1r} (0,1,0,1,1,1,0,1,1,0,1,1,0,1,1,0)$	5,10,14	6,8,9,11,13	$2^{-28.5}$
$(0,0,0,0,1,1,0,1,1,1,1,0,1,1,0,1) \xrightarrow{1r} (1,0,1,0,0,0,1,0,0,1,0,0,1,0,0,0)$	5,10,14,16,17,18	6,8,9,11,13,17,18	2^{-12}
$(0,0,0,0,1,1,0,1,1,1,1,0,1,1,1,0) \xrightarrow{1r} (1,0,0,1,1,1,0,0,1,0,1,1,0,1,1,0)$	5,10,14,18	6,8,9,11,13,15,18	$2^{-28.5}$
$(0,0,0,0,1,1,0,1,1,1,1,0,1,1,1,1) \xrightarrow{1r} (0,1,1,0,0,0,1,1,0,1,0,0,1,0,0,0)$	5,10,14,16,17	6,8,9,11,13,15,17	2^{-12}
$(0,0,0,0,1,1,0,1,1,1,1,1,0,0,0,0) \xrightarrow{1r} (1,0,0,0,1,0,1,1,1,1,0,1,0,1,1,0)$	5,10,12,18	6,8,9,11,18	2^{-12}
$(0,0,0,0,1,1,0,1,1,1,1,1,0,0,0,1) \xrightarrow{1r} (0,1,1,1,0,1,0,0,0,0,1,0,1,0,0,0)$	5,10,12,16,17	6,8,9,11,17	$2^{-6.5}$
$(0,0,0,0,1,1,0,1,1,1,1,1,0,0,1,0) \xrightarrow{1r} (0,1,0,0,1,0,1,0,1,1,0,1,1,0,1,1,0)$	5,10,12	6,8,9,11,15	2^{-12}
$(0,0,0,0,1,1,0,1,1,1,1,1,0,0,1,1) \xrightarrow{1r} (1,0,1,1,0,1,0,1,0,0,1,0,1,0,0,0)$	5,10,12,16,17,18	6,8,9,11,15,17,18	$2^{-6.5}$
$(0,0,0,0,1,1,0,1,1,1,1,1,0,1,0,0) \xrightarrow{1r} (0,1,0,1,0,1,1,0,1,0,1,0,1,0,0,1)$	5,10,12,14,17	6,8,9,11,17	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,1,1,1,0,1,0,1) \xrightarrow{1r} (1,0,1,0,1,0,0,1,0,1,0,1,0,1,1,1)$	5,10,12,14,16,18	6,8,9,11,18	2^{-12}
$(0,0,0,0,1,1,0,1,1,1,1,1,0,1,1,0) \xrightarrow{1r} (1,0,0,1,0,1,1,1,1,0,1,0,1,0,0,1)$	5,10,12,14,17,18	6,8,9,11,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,1,1,1,0,1,1,1) \xrightarrow{1r} (0,1,1,0,1,0,0,0,0,1,0,1,0,1,1,1)$	5,10,12,14,16	6,8,9,11,15	2^{-12}
$(0,0,0,0,1,1,0,1,1,1,1,1,1,0,0,0) \xrightarrow{1r} (0,1,0,1,1,1,1,1,1,0,0,1,0,1,1,0)$	5,10,12	6,8,9,11,13	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,1,1,1,1,0,0,1) \xrightarrow{1r} (1,0,1,0,0,0,0,0,0,1,1,0,1,0,0,0)$	5,10,12,16,17,18	6,8,9,11,13,17,18	2^{-12}
$(0,0,0,0,1,1,0,1,1,1,1,1,1,0,1,0) \xrightarrow{1r} (1,0,0,1,1,1,1,0,1,0,0,1,0,1,1,0)$	5,10,12,18	6,8,9,11,13,15,18	$2^{-17.5}$
$(0,0,0,0,1,1,0,1,1,1,1,1,1,0,1,1) \xrightarrow{1r} (0,1,1,0,0,0,0,1,0,1,1,0,1,0,0,0)$	5,10,12,16,17	6,8,9,11,13,15,17	2^{-12}
$(0,0,0,0,1,1,0,1,1,1,1,1,1,1,0,0) \xrightarrow{1r} (1,0,0,0,0,0,1,0,1,1,1,0,1,0,0,1)$	5,10,12,14,17,18	6,8,9,11,13,17,18	2^{-12}
$(0,0,0,0,1,1,0,1,1,1,1,1,1,1,0,1) \xrightarrow{1r} (0,1,1,1,1,1,0,1,0,0,0,1,0,1,1,1)$	5,10,12,14,16	6,8,9,11,13	$2^{-6.5}$
$(0,0,0,0,1,1,0,1,1,1,1,1,1,1,1,0) \xrightarrow{1r} (0,1,0,0,0,0,1,1,1,1,1,0,1,0,0,1)$	5,10,12,14,17	6,8,9,11,13,15,17	2^{-12}
$(0,0,0,0,1,1,0,1,1,1,1,1,1,1,1,1) \xrightarrow{1r} (1,0,1,1,1,1,0,0,0,0,0,1,0,1,1,1)$	5,10,12,14,16,18	6,8,9,11,13,15,18	$2^{-6.5}$

Table 0.113 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,1,1,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (1,1,0,0,1,1,1,1,0,0,1,0,0,0,1,1)$	5,7,17,18	6,17,18	2^{-12}
$(0,0,0,0,1,1,1,0,0,0,0,0,0,0,0,1) \xrightarrow{1r} (0,0,1,1,0,0,0,0,1,1,0,1,1,1,0,1)$	5,7,16	6	$2^{-6.5}$
$(0,0,0,0,1,1,1,0,0,0,0,0,0,0,1,0) \xrightarrow{1r} (0,0,0,0,1,1,1,0,0,0,1,0,0,0,1,1)$	5,7,17	6,15,17	2^{-12}
$(0,0,0,0,1,1,1,0,0,0,0,0,0,0,1,1) \xrightarrow{1r} (1,1,1,1,0,0,0,1,1,1,0,1,1,1,0,1)$	5,7,16,18	6,15,18	$2^{-6.5}$
$(0,0,0,0,1,1,1,0,0,0,0,0,0,1,0,0) \xrightarrow{1r} (0,0,0,1,0,0,1,0,0,1,0,1,1,1,0,0)$	5,7,14	6	$2^{-6.5}$
$(0,0,0,0,1,1,1,0,0,0,0,0,0,1,0,1) \xrightarrow{1r} (1,1,1,0,1,1,0,1,1,0,1,0,0,0,1,0)$	5,7,14,16,17,18	6,17,18	2^{-23}
$(0,0,0,0,1,1,1,0,0,0,0,0,0,1,1,0) \xrightarrow{1r} (1,1,0,1,0,0,1,1,0,1,0,1,1,1,0,0)$	5,7,14,18	6,15,18	$2^{-6.5}$
$(0,0,0,0,1,1,1,0,0,0,0,0,0,1,1,1) \xrightarrow{1r} (0,0,1,0,1,1,0,0,1,0,1,0,0,0,1,0)$	5,7,14,16,17	6,15,17	2^{-23}
$(0,0,0,0,1,1,1,0,0,0,0,0,0,1,0,0) \xrightarrow{1r} (0,0,0,1,1,0,1,1,0,1,1,0,0,0,1,1)$	5,7,17	6,13,17	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,0,0,0,0,0,1,0,1) \xrightarrow{1r} (1,1,1,0,0,1,0,0,1,0,0,1,1,1,0,1)$	5,7,16,18	6,13,18	2^{-12}
$(0,0,0,0,1,1,1,0,0,0,0,0,0,1,0,1) \xrightarrow{1r} (1,1,0,1,1,0,1,0,0,1,1,0,0,0,1,1)$	5,7,17,18	6,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,0,0,0,0,0,1,0,1) \xrightarrow{1r} (0,0,1,0,0,1,0,1,1,0,0,1,1,1,0,1)$	5,7,16	6,13,15	2^{-12}
$(0,0,0,0,1,1,1,0,0,0,0,0,0,1,1,0) \xrightarrow{1r} (1,1,0,0,0,1,1,0,0,0,0,1,1,1,0,0)$	5,7,14,18	6,13,18	2^{-1}
$(0,0,0,0,1,1,1,0,0,0,0,0,0,1,1,0) \xrightarrow{1r} (0,0,1,1,1,0,0,1,1,1,1,0,0,0,1,0)$	5,7,14,16,17	6,13,17	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,0,0,0,0,0,1,1,1) \xrightarrow{1r} (0,0,0,0,0,1,1,1,0,0,0,1,1,1,0,0)$	5,7,14	6,13,15	2^{-1}
$(0,0,0,0,1,1,1,0,0,0,0,0,0,1,1,1) \xrightarrow{1r} (1,1,1,1,1,0,0,0,1,1,1,0,0,0,1,0)$	5,7,14,16,17,18	6,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,0,0,0,0,1,0,0,0) \xrightarrow{1r} (0,0,0,1,0,0,0,0,0,0,1,1,1,1,0,0)$	5,7,12	6	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,0,0,0,0,1,0,0,0) \xrightarrow{1r} (1,1,1,0,1,1,1,1,1,0,0,0,0,0,1,0)$	5,7,12,16,17,18	6,17,18	2^{-23}
$(0,0,0,0,1,1,1,0,0,0,0,0,1,0,0,1) \xrightarrow{1r} (1,1,0,1,0,0,0,1,0,1,1,1,1,1,0,0)$	5,7,12,18	6,15,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,0,0,0,0,1,0,0,1) \xrightarrow{1r} (0,0,1,0,1,1,1,0,1,0,0,0,0,0,1,0)$	5,7,12,16,17	6,15,17	2^{-23}
$(0,0,0,0,1,1,1,0,0,0,0,0,1,0,1,0) \xrightarrow{1r} (1,1,0,0,1,1,0,1,0,0,0,0,0,0,1,1)$	5,7,12,14,17,18	6,17,18	2^{-12}
$(0,0,0,0,1,1,1,0,0,0,0,0,1,0,1,0) \xrightarrow{1r} (0,0,1,1,0,0,1,0,1,1,1,1,1,1,0,1)$	5,7,12,14,16	6	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,0,0,0,0,1,0,1,1) \xrightarrow{1r} (0,0,0,0,1,1,0,0,0,0,0,0,0,0,1,1)$	5,7,12,14,17	6,15,17	2^{-12}
$(0,0,0,0,1,1,1,0,0,0,0,0,1,0,1,1) \xrightarrow{1r} (1,1,1,1,0,0,1,1,1,1,1,1,1,1,0,1)$	5,7,12,14,16,18	6,15,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,0,0,0,0,1,1,0,0) \xrightarrow{1r} (1,1,0,0,0,1,0,0,0,0,1,1,1,1,0,0)$	5,7,12,18	6,13,18	2^{-12}
$(0,0,0,0,1,1,1,0,0,0,0,0,1,1,0,0) \xrightarrow{1r} (0,0,1,1,1,0,1,1,1,1,0,0,0,0,1,0)$	5,7,12,16,17	6,13,17	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,0,0,0,0,1,1,0,1) \xrightarrow{1r} (0,0,0,0,0,1,0,1,0,0,0,1,1,1,0,0)$	5,7,12	6,13,15	2^{-12}
$(0,0,0,0,1,1,1,0,0,0,0,0,1,1,0,1) \xrightarrow{1r} (1,1,1,1,1,0,1,0,1,1,0,0,0,0,1,0)$	5,7,12,16,17,18	6,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,0,0,0,0,1,1,1,0) \xrightarrow{1r} (0,0,0,1,1,0,0,1,0,1,0,0,0,0,1,1)$	5,7,12,14,17	6,13,17	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,0,0,0,0,1,1,1,0) \xrightarrow{1r} (1,1,1,0,0,1,1,0,1,0,1,1,1,1,0,1)$	5,7,12,14,16,18	6,13,18	2^{-23}
$(0,0,0,0,1,1,1,0,0,0,0,0,1,1,1,1) \xrightarrow{1r} (1,1,0,1,1,0,0,0,0,1,0,0,0,0,1,1)$	5,7,12,14,17,18	6,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,0,0,0,0,1,1,1,1) \xrightarrow{1r} (0,0,1,0,0,1,1,1,1,0,1,1,1,1,0,1)$	5,7,12,14,16	6,13,15	2^{-23}

Table 0.114 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,1,1,0,0,0,1,0,0,0,0,0) \xrightarrow{1r} (0,0,0,0,1,0,1,1,0,1,1,1,0,0,1,1)$	5,7,17	6,11,17	2^{-23}
$(0,0,0,0,1,1,1,0,0,0,1,0,0,0,0,1) \xrightarrow{1r} (1,1,1,1,0,1,0,0,1,0,0,0,1,1,0,1)$	5,7,16,18	6,11,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,0,0,1,0,0,0,1,0) \xrightarrow{1r} (1,1,0,0,1,0,1,0,0,1,1,1,0,0,1,1)$	5,7,17,18	6,11,15,17,18	2^{-23}
$(0,0,0,0,1,1,1,0,0,0,1,0,0,0,1,1) \xrightarrow{1r} (0,0,1,1,0,1,0,1,1,0,0,0,1,1,0,1)$	5,7,16	6,11,15	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,0,0,1,0,0,1,0,0) \xrightarrow{1r} (1,1,0,1,0,1,1,0,0,0,0,0,1,1,0,0)$	5,7,14,18	6,11,18	$2^{-6.5}$
$(0,0,0,0,1,1,1,0,0,0,1,0,0,1,0,1) \xrightarrow{1r} (0,0,1,0,1,0,0,1,1,1,1,1,0,0,1,0)$	5,7,14,16,17	6,11,17	2^{-23}
$(0,0,0,0,1,1,1,0,0,0,1,0,0,1,1,0) \xrightarrow{1r} (0,0,0,1,0,1,1,1,0,0,0,0,1,1,0,0)$	5,7,14	6,11,15	$2^{-6.5}$
$(0,0,0,0,1,1,1,0,0,0,1,0,0,1,1,1) \xrightarrow{1r} (1,1,1,0,1,0,0,0,1,1,1,1,0,0,1,0)$	5,7,14,16,17,18	6,11,15,17,18	2^{-23}
$(0,0,0,0,1,1,1,0,0,0,1,0,1,0,0,0) \xrightarrow{1r} (1,1,0,1,1,1,1,0,0,1,1,0,0,1,1)$	5,7,17,18	6,11,13,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,0,0,1,0,1,0,0,1) \xrightarrow{1r} (0,0,1,0,0,0,0,0,1,1,0,0,1,1,0,1)$	5,7,16	6,11,13	2^{-12}
$(0,0,0,0,1,1,1,0,0,0,1,0,1,0,1,0) \xrightarrow{1r} (0,0,0,1,1,1,1,0,0,0,1,1,0,0,1,1)$	5,7,17	6,11,13,15,17	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,0,0,1,0,1,0,1,1) \xrightarrow{1r} (1,1,1,0,0,0,0,1,1,1,0,0,1,1,0,1)$	5,7,16,18	6,11,13,15,18	2^{-12}
$(0,0,0,0,1,1,1,0,0,0,1,0,1,1,0,0) \xrightarrow{1r} (0,0,0,0,0,0,1,0,0,1,0,0,1,1,0,0)$	5,7,14	6,11,13	2^{-12}
$(0,0,0,0,1,1,1,0,0,0,1,0,1,1,0,1) \xrightarrow{1r} (1,1,1,1,1,1,0,1,1,0,1,1,0,0,1,0)$	5,7,14,16,17,18	6,11,13,17,18	$2^{-28.5}$
$(0,0,0,0,1,1,1,0,0,0,1,0,1,1,1,0) \xrightarrow{1r} (1,1,0,0,0,0,1,1,0,1,0,0,1,1,0,0)$	5,7,14,18	6,11,13,15,18	2^{-12}
$(0,0,0,0,1,1,1,0,0,0,1,0,1,1,1,1) \xrightarrow{1r} (0,0,1,1,1,1,0,0,1,0,1,1,0,0,1,0)$	5,7,14,16,17	6,11,13,15,17	$2^{-28.5}$
$(0,0,0,0,1,1,1,0,0,0,1,1,0,0,0,0) \xrightarrow{1r} (1,1,0,1,0,1,0,0,0,0,1,0,1,1,0,0)$	5,7,12,18	6,11,18	$2^{-6.5}$
$(0,0,0,0,1,1,1,0,0,0,1,1,0,0,0,1) \xrightarrow{1r} (0,0,1,0,1,0,1,1,1,1,0,1,0,0,1,0)$	5,7,12,16,17	6,11,17	2^{-12}
$(0,0,0,0,1,1,1,0,0,0,1,1,0,0,1,0) \xrightarrow{1r} (0,0,0,1,0,1,0,1,0,0,1,0,1,1,0,0)$	5,7,12	6,11,15	$2^{-6.5}$
$(0,0,0,0,1,1,1,0,0,0,1,1,0,0,1,1) \xrightarrow{1r} (1,1,1,0,1,0,1,0,1,1,0,1,0,0,1,0)$	5,7,12,16,17,18	6,11,15,17,18	2^{-12}
$(0,0,0,0,1,1,1,0,0,0,1,1,0,1,0,0) \xrightarrow{1r} (0,0,0,0,1,0,0,1,0,1,0,1,0,0,1,1)$	5,7,12,14,17	6,11,17	2^{-12}
$(0,0,0,0,1,1,1,0,0,0,1,1,0,1,0,1) \xrightarrow{1r} (1,1,1,1,0,1,1,0,1,0,1,0,1,1,0,1)$	5,7,12,14,16,18	6,11,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,0,0,1,1,0,1,1,0) \xrightarrow{1r} (1,1,0,0,1,0,0,0,0,1,0,1,0,0,1,1)$	5,7,12,14,17,18	6,11,15,17,18	2^{-12}
$(0,0,0,0,1,1,1,0,0,0,1,1,0,1,1,1) \xrightarrow{1r} (0,0,1,1,0,1,1,1,1,0,1,0,1,1,0,1)$	5,7,12,14,16	6,11,15	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,0,0,1,1,1,0,0,0) \xrightarrow{1r} (0,0,0,0,0,0,0,0,0,1,1,0,1,1,0,0)$	5,7,12	6,11,13	2^{-12}
$(0,0,0,0,1,1,1,0,0,0,1,1,1,0,0,1) \xrightarrow{1r} (1,1,1,1,1,1,1,1,1,0,0,1,0,0,1,0)$	5,7,12,16,17,18	6,11,13,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,0,0,1,1,1,0,1,0) \xrightarrow{1r} (1,1,0,0,0,0,0,1,0,1,1,0,1,1,0,0)$	5,7,12,18	6,11,13,15,18	2^{-12}
$(0,0,0,0,1,1,1,0,0,0,1,1,1,0,1,1) \xrightarrow{1r} (0,0,1,1,1,1,1,0,1,0,0,1,0,0,1,0)$	5,7,12,16,17	6,11,13,15,17	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,0,0,1,1,1,1,0,0) \xrightarrow{1r} (1,1,0,1,1,1,0,1,0,0,0,1,0,0,1,1)$	5,7,12,14,17,18	6,11,13,17,18	$2^{-6.5}$
$(0,0,0,0,1,1,1,0,0,0,1,1,1,1,0,1) \xrightarrow{1r} (0,0,1,0,0,0,1,0,1,1,1,0,1,1,0,1)$	5,7,12,14,16	6,11,13	2^{-12}
$(0,0,0,0,1,1,1,0,0,0,1,1,1,1,1,0) \xrightarrow{1r} (0,0,0,1,1,1,0,0,0,0,0,1,0,0,1,1)$	5,7,12,14,17	6,11,13,15,17	$2^{-6.5}$
$(0,0,0,0,1,1,1,0,0,0,1,1,1,1,1,1) \xrightarrow{1r} (1,1,1,0,0,0,1,1,1,1,0,1,1,0,1,0)$	5,7,12,14,16,18	6,11,13,15,18	2^{-12}

Table 0.115 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	5,7,10	6	$2^{-28.5}$
$(0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	5,7,10,16,17,18	6,17,18	2^{-23}
$(0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	5,7,10,18	6,15,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	5,7,10,16,17	6,15,17	2^{-23}
$(0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	5,7,10,14,17,18	6,17,18	2^{-12}
$(0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	5,7,10,14,16	6	$2^{-28.5}$
$(0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	5,7,10,14,17	6,15,17	2^{-12}
$(0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	5,7,10,14,16,18	6,15,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	5,7,10,18	6,13,18	2^{-23}
$(0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	5,7,10,16,17	6,13,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	5,7,10	6,13,15	2^{-23}
$(0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	5,7,10,16,17,18	6,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	5,7,10,14,17	6,13,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	5,7,10,14,16,18	6,13,18	2^{-34}
$(0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	5,7,10,14,17,18	6,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	5,7,10,14,16	6,13,15	2^{-34}
$(0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	5,7,10,12,17,18	6,17,18	2^{-12}
$(0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	5,7,10,12,16	6	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	5,7,10,12,17	6,15,17	2^{-12}
$(0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	5,7,10,12,16,18	6,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	5,7,10,12,14	6	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	5,7,10,12,14,16,17,18	6,17,18	2^{-23}
$(0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	5,7,10,12,14,18	6,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	5,7,10,12,14,16,17	6,15,17	2^{-23}
$(0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	5,7,10,12,17	6,13,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	5,7,10,12,16,18	6,13,18	2^{-23}
$(0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	5,7,10,12,17,18	6,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	5,7,10,12,16	6,13,15	2^{-23}
$(0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	5,7,10,12,14,18	6,13,18	2^{-12}
$(0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	5,7,10,12,14,16,17	6,13,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	5,7,10,12,14	6,13,15	2^{-12}
$(0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	5,7,10,12,14,16,17,18	6,13,15,17,18	$2^{-17.5}$

Table 0.116 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,1,1,0,0,1,1,0,0,0,0,0) \xrightarrow{1r} (1,1,1,1,1,1,1,0,0,0,1,0,0,1,0,0)$	5,7,10,18	6,11,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,0,1,1,0,0,0,0,1) \xrightarrow{1r} (0,0,0,0,0,0,0,1,1,1,0,1,1,0,1,0)$	5,7,10,16,17	6,11,17	2^{-12}
$(0,0,0,0,1,1,1,0,0,1,1,0,0,0,1,0) \xrightarrow{1r} (0,0,1,1,1,1,1,0,0,1,0,0,1,0,0,0)$	5,7,10	6,11,15	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,0,1,1,0,0,0,1,1) \xrightarrow{1r} (1,1,0,0,0,0,0,0,1,1,0,1,1,0,1,0)$	5,7,10,16,17,18	6,11,15,17,18	2^{-12}
$(0,0,0,0,1,1,1,0,0,1,1,0,0,1,0,0) \xrightarrow{1r} (0,0,1,0,0,0,1,1,0,1,0,1,1,0,1,1)$	5,7,10,14,17	6,11,17	2^{-12}
$(0,0,0,0,1,1,1,0,0,1,1,0,0,1,0,1) \xrightarrow{1r} (1,1,0,1,1,1,0,0,1,0,1,0,0,1,0,1)$	5,7,10,14,16,18	6,11,18	$2^{-28.5}$
$(0,0,0,0,1,1,1,0,0,1,1,0,0,1,1,0) \xrightarrow{1r} (1,1,1,0,0,0,1,0,0,1,0,1,1,0,1,1)$	5,7,10,14,17,18	6,11,15,17,18	2^{-12}
$(0,0,0,0,1,1,1,0,0,1,1,0,0,1,1,1) \xrightarrow{1r} (0,0,0,1,1,1,0,1,1,0,1,0,0,1,0,1)$	5,7,10,14,16	6,11,15	$2^{-28.5}$
$(0,0,0,0,1,1,1,0,0,1,1,0,1,0,0,0) \xrightarrow{1r} (0,0,1,0,1,0,1,0,0,1,1,0,0,1,0,0)$	5,7,10	6,11,13	2^{-23}
$(0,0,0,0,1,1,1,0,0,1,1,0,1,0,0,1) \xrightarrow{1r} (1,1,0,1,0,1,0,1,1,0,0,1,1,0,1,0)$	5,7,10,16,17,18	6,11,13,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,0,1,1,0,1,0,1,0) \xrightarrow{1r} (1,1,1,0,1,0,1,1,0,1,1,0,0,1,0,0)$	5,7,10,18	6,11,13,15,18	2^{-23}
$(0,0,0,0,1,1,1,0,0,1,1,0,1,0,1,1) \xrightarrow{1r} (0,0,0,1,0,1,0,0,1,0,0,1,1,0,1,0)$	5,7,10,16,17	6,11,13,15,17	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,0,1,1,0,1,1,0,0) \xrightarrow{1r} (1,1,1,1,0,1,1,1,0,0,0,1,1,0,1,1)$	5,7,10,14,17,18	6,11,13,17,18	$2^{-6.5}$
$(0,0,0,0,1,1,1,0,0,1,1,0,1,1,0,1) \xrightarrow{1r} (0,0,0,0,1,0,0,0,1,1,1,0,0,1,0,1)$	5,7,10,14,16	6,11,13	2^{-23}
$(0,0,0,0,1,1,1,0,0,1,1,0,1,1,1,0) \xrightarrow{1r} (0,0,1,1,0,1,1,0,0,0,0,1,1,0,1,1)$	5,7,10,14,17	6,11,13,15,17	$2^{-6.5}$
$(0,0,0,0,1,1,1,0,0,1,1,0,1,1,1,1) \xrightarrow{1r} (1,1,0,0,1,0,0,1,1,1,1,0,0,1,0,1)$	5,7,10,14,16,18	6,11,13,15,18	2^{-23}
$(0,0,0,0,1,1,1,0,0,1,1,1,0,0,0,0) \xrightarrow{1r} (0,0,1,0,0,0,0,1,0,1,1,1,1,0,1,1)$	5,7,10,12,17	6,11,17	2^{-23}
$(0,0,0,0,1,1,1,0,0,1,1,1,0,0,0,1) \xrightarrow{1r} (1,1,0,1,1,1,1,0,1,0,0,0,0,1,0,1)$	5,7,10,12,16,18	6,11,18	$2^{-28.5}$
$(0,0,0,0,1,1,1,0,0,1,1,1,0,0,1,0) \xrightarrow{1r} (1,1,1,0,0,0,0,0,0,1,1,1,1,0,1,1)$	5,7,10,12,17,18	6,11,15,17,18	2^{-23}
$(0,0,0,0,1,1,1,0,0,1,1,1,0,0,1,1) \xrightarrow{1r} (0,0,0,1,1,1,1,1,1,0,0,0,0,1,0,1)$	5,7,10,12,16	6,11,15	$2^{-28.5}$
$(0,0,0,0,1,1,1,0,0,1,1,1,0,1,0,0) \xrightarrow{1r} (1,1,1,1,1,1,0,0,0,0,0,0,0,1,0,0)$	5,7,10,12,14,18	6,11,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,0,1,1,1,0,1,0,1) \xrightarrow{1r} (0,0,0,0,0,0,1,1,1,1,1,1,0,1,0)$	5,7,10,12,14,16,17	6,11,17	2^{-23}
$(0,0,0,0,1,1,1,0,0,1,1,1,0,1,1,0) \xrightarrow{1r} (0,0,1,1,1,1,0,1,0,0,0,0,0,1,0,0)$	5,7,10,12,14	6,11,15	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,0,1,1,1,0,1,1,1) \xrightarrow{1r} (1,1,0,0,0,0,1,0,1,1,1,1,1,0,1,0)$	5,7,10,12,14,16,17,18	6,11,15,17,18	2^{-23}
$(0,0,0,0,1,1,1,0,0,1,1,1,1,0,0,0) \xrightarrow{1r} (1,1,1,1,0,1,0,1,0,0,1,1,1,0,1,1)$	5,7,10,12,17,18	6,11,13,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,0,1,1,1,1,0,0,1) \xrightarrow{1r} (0,0,0,0,1,0,1,0,1,1,1,0,0,0,1,0,1)$	5,7,10,12,16	6,11,13	2^{-23}
$(0,0,0,0,1,1,1,0,0,1,1,1,1,0,1,0) \xrightarrow{1r} (0,0,1,1,0,1,0,0,0,0,1,1,1,0,1,1)$	5,7,10,12,17	6,11,13,15,17	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,0,1,1,1,1,0,1,1) \xrightarrow{1r} (1,1,0,0,1,0,1,1,1,1,0,0,0,1,0,1)$	5,7,10,12,16,18	6,11,13,15,18	2^{-23}
$(0,0,0,0,1,1,1,0,0,1,1,1,1,1,0,0) \xrightarrow{1r} (0,0,1,0,1,0,0,0,0,1,0,0,0,1,0,0)$	5,7,10,12,14	6,11,13	2^{-23}
$(0,0,0,0,1,1,1,0,0,1,1,1,1,1,0,1) \xrightarrow{1r} (1,1,0,1,0,1,1,1,1,0,1,1,1,0,1,0)$	5,7,10,12,14,16,17,18	6,11,13,17,18	$2^{-28.5}$
$(0,0,0,0,1,1,1,0,0,1,1,1,1,1,1,0) \xrightarrow{1r} (1,1,1,0,1,0,0,1,0,1,0,0,0,1,0,0)$	5,7,10,12,14,18	6,11,13,15,18	2^{-23}
$(0,0,0,0,1,1,1,0,0,1,1,1,1,1,1,1) \xrightarrow{1r} (0,0,0,1,0,1,1,0,1,0,1,1,1,0,1,0)$	5,7,10,12,14,16,17	6,11,13,15,17	$2^{-28.5}$

Table 0.117 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,1,1,0,1,0,0,0,0,0,0,0) \xrightarrow{1r} (0,1,0,1,1,0,1,0,0,1,1,1,0,1,1,1)$	5,7,17	6,9,17	$2^{-28.5}$
$(0,0,0,0,1,1,1,0,1,0,0,0,0,0,0,1) \xrightarrow{1r} (1,0,1,0,0,1,0,1,1,0,0,0,1,0,0,1)$	5,7,16,18	6,9,18	2^{-23}
$(0,0,0,0,1,1,1,0,1,0,0,0,0,0,1,0) \xrightarrow{1r} (1,0,0,1,1,0,1,1,0,1,1,1,0,1,1,1)$	5,7,17,18	6,9,15,17,18	$2^{-28.5}$
$(0,0,0,0,1,1,1,0,1,0,0,0,0,0,1,1) \xrightarrow{1r} (0,1,1,0,0,1,0,0,1,0,0,0,1,0,0,1)$	5,7,16	6,9,15	2^{-23}
$(0,0,0,0,1,1,1,0,1,0,0,0,0,1,0,0) \xrightarrow{1r} (1,0,0,0,0,1,1,1,0,0,0,0,1,0,0,0)$	5,7,14,18	6,9,18	2^{-12}
$(0,0,0,0,1,1,1,0,1,0,0,0,0,1,0,1) \xrightarrow{1r} (0,1,1,1,0,0,0,1,1,1,1,0,1,1,0,1)$	5,7,14,16,17	6,9,17	$2^{-28.5}$
$(0,0,0,0,1,1,1,0,1,0,0,0,0,1,1,0) \xrightarrow{1r} (0,1,0,0,0,1,1,0,0,0,0,0,1,0,0,0)$	5,7,14	6,9,15	2^{-12}
$(0,0,0,0,1,1,1,0,1,0,0,0,0,1,1,1) \xrightarrow{1r} (1,0,1,1,1,0,0,1,1,1,1,1,0,1,1,0)$	5,7,14,16,17,18	6,9,15,17,18	$2^{-28.5}$
$(0,0,0,0,1,1,1,0,1,0,0,0,1,0,0,0) \xrightarrow{1r} (1,0,0,0,1,1,1,0,0,0,1,1,0,1,1,1)$	5,7,17,18	6,9,13,17,18	2^{-23}
$(0,0,0,0,1,1,1,0,1,0,0,0,1,0,0,1) \xrightarrow{1r} (0,1,1,1,0,0,0,1,1,1,0,0,1,0,0,1)$	5,7,16	6,9,13	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,0,0,0,1,0,1,0) \xrightarrow{1r} (0,1,0,0,1,1,1,1,0,0,1,1,0,1,1,1)$	5,7,17	6,9,13,15,17	2^{-23}
$(0,0,0,0,1,1,1,0,1,0,0,0,1,0,1,1) \xrightarrow{1r} (1,0,1,1,0,0,0,0,1,1,0,0,1,0,0,1)$	5,7,16,18	6,9,13,15,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,0,0,0,1,1,0,0) \xrightarrow{1r} (0,1,0,1,0,0,1,1,0,1,0,0,1,0,0,0)$	5,7,14	6,9,13	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,0,0,0,1,1,0,1) \xrightarrow{1r} (1,0,1,0,1,1,0,0,1,0,1,1,0,1,1,0)$	5,7,14,16,17,18	6,9,13,17,18	2^{-34}
$(0,0,0,0,1,1,1,0,1,0,0,0,1,1,1,0) \xrightarrow{1r} (1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,0)$	5,7,14,18	6,9,13,15,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,0,0,0,1,1,1,1) \xrightarrow{1r} (0,1,1,0,1,1,0,1,1,0,1,1,0,1,1,0)$	5,7,14,16,17	6,9,13,15,17	2^{-34}
$(0,0,0,0,1,1,1,0,1,0,0,1,0,0,0,0) \xrightarrow{1r} (1,0,0,0,0,1,0,1,0,0,1,0,1,0,0,0)$	5,7,12,18	6,9,18	2^{-12}
$(0,0,0,0,1,1,1,0,1,0,0,1,0,0,0,1) \xrightarrow{1r} (0,1,1,1,1,0,1,0,1,1,0,1,0,1,1,0)$	5,7,12,16,17	6,9,17	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,0,0,1,0,0,1,0) \xrightarrow{1r} (0,1,0,0,0,1,0,0,0,0,1,0,1,0,0,0)$	5,7,12	6,9,15	2^{-12}
$(0,0,0,0,1,1,1,0,1,0,0,1,0,0,1,1) \xrightarrow{1r} (1,0,1,1,1,0,1,1,1,1,0,1,0,1,1,0)$	5,7,12,16,17,18	6,9,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,0,0,1,0,1,0,0) \xrightarrow{1r} (0,1,0,1,1,0,0,0,0,1,0,1,0,1,1,1)$	5,7,12,14,17	6,9,17	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,0,0,1,0,1,0,1) \xrightarrow{1r} (1,0,1,0,0,1,1,1,1,0,1,0,1,0,0,1)$	5,7,12,14,16,18	6,9,18	2^{-23}
$(0,0,0,0,1,1,1,0,1,0,0,1,0,1,1,0) \xrightarrow{1r} (1,0,0,1,1,0,0,1,0,1,0,1,0,1,1,1)$	5,7,12,14,17,18	6,9,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,0,0,1,0,1,1,1) \xrightarrow{1r} (0,1,1,0,0,1,1,0,1,0,1,0,1,0,0,1)$	5,7,12,14,16	6,9,15	2^{-23}
$(0,0,0,0,1,1,1,0,1,0,0,1,1,0,0,0) \xrightarrow{1r} (0,1,0,1,0,0,0,1,0,1,1,0,1,0,0,0)$	5,7,12	6,9,13	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,0,0,1,1,0,0,1) \xrightarrow{1r} (1,0,1,0,1,1,1,1,0,1,0,0,1,0,1,1,0)$	5,7,12,16,17,18	6,9,13,17,18	2^{-23}
$(0,0,0,0,1,1,1,0,1,0,0,1,1,0,1,0) \xrightarrow{1r} (1,0,0,1,0,0,0,0,0,1,1,0,1,0,0,0)$	5,7,12,18	6,9,13,15,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,0,0,1,1,0,1,1) \xrightarrow{1r} (0,1,1,0,1,1,1,1,1,0,0,1,0,1,1,0)$	5,7,12,16,17	6,9,13,15,17	2^{-23}
$(0,0,0,0,1,1,1,0,1,0,0,1,1,1,0,0) \xrightarrow{1r} (1,0,0,0,1,1,0,0,0,0,0,1,0,1,1,1)$	5,7,12,14,17,18	6,9,13,17,18	2^{-12}
$(0,0,0,0,1,1,1,0,1,0,0,1,1,1,0,1) \xrightarrow{1r} (0,1,1,1,0,0,1,1,1,1,1,0,1,0,0,1)$	5,7,12,14,16	6,9,13	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,0,0,1,1,1,1,0) \xrightarrow{1r} (0,1,0,0,1,1,0,1,0,0,0,1,0,1,1,1)$	5,7,12,14,17	6,9,13,15,17	2^{-12}
$(0,0,0,0,1,1,1,0,1,0,0,1,1,1,1,1) \xrightarrow{1r} (1,0,1,1,0,0,1,0,1,1,1,0,1,0,0,1)$	5,7,12,14,16,18	6,9,13,15,18	$2^{-17.5}$

Table 0.118 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,1,1,0,1,0,1,0,0,0,0,0) \xrightarrow{1r} (1,0,0,1,1,1,1,0,0,0,1,0,0,1,1,1)$	5,7,17,18	6,9,11,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,0,1,0,0,0,0,1) \xrightarrow{1r} (0,1,1,0,0,0,0,1,1,1,0,1,1,0,0,1)$	5,7,16	6,9,11	2^{-12}
$(0,0,0,0,1,1,1,0,1,0,1,0,0,0,1,0) \xrightarrow{1r} (0,1,0,1,1,1,1,1,0,0,1,0,0,1,1,1)$	5,7,17	6,9,11,15,17	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,0,1,0,0,0,1,1) \xrightarrow{1r} (1,0,1,0,0,0,0,0,1,1,0,1,1,0,0,1)$	5,7,16,18	6,9,11,15,18	2^{-12}
$(0,0,0,0,1,1,1,0,1,0,1,0,0,1,0,0) \xrightarrow{1r} (0,1,0,0,0,0,1,1,0,1,0,1,1,0,0,0)$	5,7,14	6,9,11	2^{-12}
$(0,0,0,0,1,1,1,0,1,0,1,0,0,1,0,1) \xrightarrow{1r} (1,0,1,1,1,1,0,0,1,0,1,0,0,1,1,0)$	5,7,14,16,17,18	6,9,11,17,18	$2^{-28.5}$
$(0,0,0,0,1,1,1,0,1,0,1,0,0,1,1,0) \xrightarrow{1r} (1,0,0,0,0,0,1,0,0,1,0,1,1,0,0,0)$	5,7,14,18	6,9,11,15,18	2^{-12}
$(0,0,0,0,1,1,1,0,1,0,1,0,0,1,1,1) \xrightarrow{1r} (0,1,1,1,1,1,0,1,1,0,1,0,0,1,1,0)$	5,7,14,16,17	6,9,11,15,17	$2^{-28.5}$
$(0,0,0,0,1,1,1,0,1,0,1,0,1,0,0,0) \xrightarrow{1r} (0,1,0,0,1,0,1,0,0,1,1,0,0,1,1,1)$	5,7,17	6,9,11,13,17	2^{-23}
$(0,0,0,0,1,1,1,0,1,0,1,0,1,0,0,1) \xrightarrow{1r} (1,0,1,1,0,1,0,1,1,0,0,1,1,0,0,1)$	5,7,16,18	6,9,11,13,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,0,1,0,1,0,1,0) \xrightarrow{1r} (1,0,0,0,1,0,1,1,0,1,1,0,0,1,1,1)$	5,7,17,18	6,9,11,13,15,17,18	2^{-23}
$(0,0,0,0,1,1,1,0,1,0,1,0,1,0,1,1) \xrightarrow{1r} (0,1,1,1,0,1,0,0,1,0,0,1,1,0,0,1)$	5,7,16	6,9,11,13,15	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,0,1,0,1,1,0,0) \xrightarrow{1r} (1,0,0,1,0,1,1,1,0,0,0,1,1,0,0,0)$	5,7,14,18	6,9,11,13,18	$2^{-6.5}$
$(0,0,0,0,1,1,1,0,1,0,1,0,1,1,0,1) \xrightarrow{1r} (0,1,1,0,1,0,0,0,1,1,1,0,0,1,1,0)$	5,7,14,16,17	6,9,11,13,17	2^{-23}
$(0,0,0,0,1,1,1,0,1,0,1,0,1,1,1,0) \xrightarrow{1r} (0,1,0,1,0,1,1,0,0,0,0,1,1,0,0,0)$	5,7,14	6,9,11,13,15	$2^{-6.5}$
$(0,0,0,0,1,1,1,0,1,0,1,0,1,1,1,1) \xrightarrow{1r} (1,0,1,0,1,0,0,1,1,1,1,0,0,1,1,0)$	5,7,14,16,17,18	6,9,11,13,15,17,18	2^{-23}
$(0,0,0,0,1,1,1,0,1,0,1,1,0,0,0,0) \xrightarrow{1r} (0,1,0,0,0,0,0,1,0,1,1,1,1,0,0,0)$	5,7,12	6,9,11	2^{-23}
$(0,0,0,0,1,1,1,0,1,0,1,1,0,0,0,1) \xrightarrow{1r} (1,0,1,1,1,1,1,0,1,0,0,0,0,1,1,0)$	5,7,12,16,17,18	6,9,11,17,18	$2^{-28.5}$
$(0,0,0,0,1,1,1,0,1,0,1,1,0,0,1,0) \xrightarrow{1r} (1,0,0,0,0,0,0,0,0,1,1,1,1,0,0,0)$	5,7,12,18	6,9,11,15,18	2^{-23}
$(0,0,0,0,1,1,1,0,1,0,1,1,0,0,1,1) \xrightarrow{1r} (0,1,1,1,1,1,1,1,0,0,0,0,1,1,0)$	5,7,12,16,17	6,9,11,15,17	$2^{-28.5}$
$(0,0,0,0,1,1,1,0,1,0,1,1,0,1,0,0) \xrightarrow{1r} (1,0,0,1,1,1,0,0,0,0,0,0,0,1,1,1)$	5,7,12,14,17,18	6,9,11,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,0,1,1,0,1,0,1) \xrightarrow{1r} (0,1,1,0,0,0,1,1,1,1,1,1,0,0,1)$	5,7,12,14,16	6,9,11	2^{-23}
$(0,0,0,0,1,1,1,0,1,0,1,1,0,1,1,0) \xrightarrow{1r} (0,1,0,1,1,1,0,1,0,0,0,0,0,1,1,1)$	5,7,12,14,17	6,9,11,15,17	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,0,1,1,0,1,1,1) \xrightarrow{1r} (1,0,1,0,0,0,1,0,1,1,1,1,1,0,0,1)$	5,7,12,14,16,18	6,9,11,15,18	2^{-23}
$(0,0,0,0,1,1,1,0,1,0,1,1,1,0,0,0) \xrightarrow{1r} (1,0,0,1,0,1,0,1,0,0,1,1,1,0,0,0)$	5,7,12,18	6,9,11,13,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,0,1,1,1,0,0,1) \xrightarrow{1r} (0,1,1,0,1,0,1,0,1,1,1,0,0,0,1,1,0)$	5,7,12,16,17	6,9,11,13,17	2^{-23}
$(0,0,0,0,1,1,1,0,1,0,1,1,1,0,1,0) \xrightarrow{1r} (0,1,0,1,0,1,0,0,0,0,1,1,1,0,0,0)$	5,7,12	6,9,11,13,15	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,0,1,1,1,0,1,1) \xrightarrow{1r} (1,0,1,0,1,0,1,1,1,1,1,0,0,0,1,1,0)$	5,7,12,16,17,18	6,9,11,13,15,17,18	2^{-23}
$(0,0,0,0,1,1,1,0,1,0,1,1,1,1,0,0) \xrightarrow{1r} (0,1,0,0,1,0,0,0,0,1,0,0,0,1,1,1)$	5,7,12,14,17	6,9,11,13,17	2^{-23}
$(0,0,0,0,1,1,1,0,1,0,1,1,1,1,0,1) \xrightarrow{1r} (1,0,1,1,0,1,1,1,1,0,1,1,1,0,0,1)$	5,7,12,14,16,18	6,9,11,13,18	$2^{-28.5}$
$(0,0,0,0,1,1,1,0,1,0,1,1,1,1,1,0) \xrightarrow{1r} (1,0,0,0,1,0,0,1,0,1,0,0,0,1,1,1)$	5,7,12,14,17,18	6,9,11,13,15,17,18	2^{-23}
$(0,0,0,0,1,1,1,0,1,0,1,1,1,1,1,1) \xrightarrow{1r} (0,1,1,1,0,1,1,0,1,0,1,1,1,0,0,1)$	5,7,12,14,16	6,9,11,13,15	$2^{-28.5}$

Table 0.119 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,1,1,0,1,1,0,0,0,0,0,0) \xrightarrow{1r} (1,0,1,0,1,1,1,1,0,0,1,0,0,0,0,0)$	5,7,10,18	6,9,18	2^{-12}
$(0,0,0,0,1,1,1,0,1,1,0,0,0,0,0,1) \xrightarrow{1r} (0,1,0,1,0,0,0,0,1,1,0,1,1,1,1,0)$	5,7,10,16,17	6,9,17	$2^{-6.5}$
$(0,0,0,0,1,1,1,0,1,1,0,0,0,0,1,0) \xrightarrow{1r} (0,1,1,0,1,1,1,0,0,0,1,0,0,0,0,0)$	5,7,10	6,9,15	2^{-12}
$(0,0,0,0,1,1,1,0,1,1,0,0,0,0,1,1) \xrightarrow{1r} (1,0,0,1,0,0,0,1,1,1,0,1,1,1,1,0)$	5,7,10,16,17,18	6,9,15,17,18	$2^{-6.5}$
$(0,0,0,0,1,1,1,0,1,1,0,0,0,1,0,0) \xrightarrow{1r} (0,1,1,1,0,0,1,0,0,1,0,1,1,1,1,1)$	5,7,10,14,17	6,9,17	$2^{-6.5}$
$(0,0,0,0,1,1,1,0,1,1,0,0,0,1,0,1) \xrightarrow{1r} (1,0,0,0,1,1,0,1,1,0,1,0,0,0,0,1)$	5,7,10,14,16,18	6,9,18	2^{-23}
$(0,0,0,0,1,1,1,0,1,1,0,0,0,1,1,0) \xrightarrow{1r} (1,0,1,1,0,0,1,1,0,1,0,1,1,1,1,1)$	5,7,10,14,17,18	6,9,15,17,18	$2^{-6.5}$
$(0,0,0,0,1,1,1,0,1,1,0,0,0,1,1,1) \xrightarrow{1r} (0,1,0,0,1,1,0,0,1,0,1,0,0,0,0,1)$	5,7,10,14,16	6,9,15	2^{-23}
$(0,0,0,0,1,1,1,0,1,1,0,0,1,0,0,0) \xrightarrow{1r} (0,1,1,1,1,0,1,1,0,1,1,0,0,0,0,0)$	5,7,10	6,9,13	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,1,0,0,1,0,0,1) \xrightarrow{1r} (1,0,0,0,0,1,0,0,1,0,0,1,1,1,1,0)$	5,7,10,16,17,18	6,9,13,17,18	2^{-12}
$(0,0,0,0,1,1,1,0,1,1,0,0,1,0,1,0) \xrightarrow{1r} (1,0,1,1,1,0,1,0,0,1,1,0,0,0,0,0)$	5,7,10,18	6,9,13,15,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,1,0,0,1,0,1,1) \xrightarrow{1r} (0,1,0,0,0,1,0,1,1,0,0,1,1,1,1,0)$	5,7,10,16,17	6,9,13,15,17	2^{-12}
$(0,0,0,0,1,1,1,0,1,1,0,0,1,1,0,0) \xrightarrow{1r} (1,0,1,0,0,1,1,0,0,0,0,1,1,1,1,1)$	5,7,10,14,17,18	6,9,13,17,18	2^{-1}
$(0,0,0,0,1,1,1,0,1,1,0,0,1,1,0,1) \xrightarrow{1r} (0,1,0,1,1,0,0,1,1,1,1,0,0,0,0,1)$	5,7,10,14,16	6,9,13	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,1,0,0,1,1,1,0) \xrightarrow{1r} (0,1,1,0,0,1,1,1,0,0,0,1,1,1,1,1)$	5,7,10,14,17	6,9,13,15,17	2^{-1}
$(0,0,0,0,1,1,1,0,1,1,0,0,1,1,1,1) \xrightarrow{1r} (1,0,0,1,1,0,0,0,1,1,1,0,0,0,0,1)$	5,7,10,14,16,18	6,9,13,15,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,1,0,1,0,0,0,0) \xrightarrow{1r} (0,1,1,1,0,0,0,0,0,1,1,1,1,1,1,1)$	5,7,10,12,17	6,9,17	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,1,0,1,0,0,0,1) \xrightarrow{1r} (1,0,0,0,1,1,1,1,1,0,0,0,0,0,0,1)$	5,7,10,12,16,18	6,9,18	2^{-23}
$(0,0,0,0,1,1,1,0,1,1,0,1,0,0,1,0) \xrightarrow{1r} (1,0,1,1,0,0,0,1,0,1,1,1,1,1,1,1)$	5,7,10,12,17,18	6,9,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,1,0,1,0,0,1,1) \xrightarrow{1r} (0,1,0,0,1,1,1,0,1,0,0,0,0,0,0,1)$	5,7,10,12,16	6,9,15	2^{-23}
$(0,0,0,0,1,1,1,0,1,1,0,1,0,1,0,0) \xrightarrow{1r} (1,0,1,0,1,1,0,1,0,0,0,0,0,0,0,0)$	5,7,10,12,14,18	6,9,18	2^{-12}
$(0,0,0,0,1,1,1,0,1,1,0,1,0,1,0,1) \xrightarrow{1r} (0,1,0,1,0,0,1,0,1,1,1,1,1,1,1,1)$	5,7,10,12,14,16,17	6,9,17	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,1,0,1,0,1,1,0) \xrightarrow{1r} (0,1,1,0,1,1,0,0,0,0,0,0,0,0,0,0)$	5,7,10,12,14	6,9,15	2^{-12}
$(0,0,0,0,1,1,1,0,1,1,0,1,0,1,1,1) \xrightarrow{1r} (1,0,0,1,0,0,1,1,1,1,1,1,1,1,1,0)$	5,7,10,12,14,16,17,18	6,9,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,1,0,1,1,0,0,0) \xrightarrow{1r} (1,0,1,0,0,1,0,0,0,0,1,1,1,1,1,1)$	5,7,10,12,17,18	6,9,13,17,18	2^{-12}
$(0,0,0,0,1,1,1,0,1,1,0,1,1,0,0,1) \xrightarrow{1r} (0,1,0,1,1,0,1,1,1,1,0,0,0,0,0,1)$	5,7,10,12,16	6,9,13	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,1,0,1,1,0,1,0) \xrightarrow{1r} (0,1,1,0,0,1,0,1,0,0,1,1,1,1,1,1)$	5,7,10,12,17	6,9,13,15,17	2^{-12}
$(0,0,0,0,1,1,1,0,1,1,0,1,1,0,1,1) \xrightarrow{1r} (1,0,0,1,1,0,1,0,1,1,0,0,0,0,0,1)$	5,7,10,12,16,18	6,9,13,15,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,1,0,1,1,1,0,0) \xrightarrow{1r} (0,1,1,1,1,0,0,1,0,1,0,0,0,0,0,0)$	5,7,10,12,14	6,9,13	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,1,0,1,1,1,0,1) \xrightarrow{1r} (1,0,0,0,0,1,1,0,1,0,1,1,1,1,1,0)$	5,7,10,12,14,16,17,18	6,9,13,17,18	2^{-23}
$(0,0,0,0,1,1,1,0,1,1,0,1,1,1,1,0) \xrightarrow{1r} (1,0,1,1,1,0,0,0,0,1,0,0,0,0,0,0)$	5,7,10,12,14,18	6,9,13,15,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,1,0,1,1,1,1,1) \xrightarrow{1r} (0,1,0,0,0,1,1,1,1,0,1,1,1,1,1,0)$	5,7,10,12,14,16,17	6,9,13,15,17	2^{-23}

Table 0.120 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,1,1,0,1,1,1,0,0,0,0,0) \xrightarrow{1r} (0,1,1,0,1,0,1,1,0,1,1,1,0,0,0,0)$	5,7,10	6,9,11	2^{-23}
$(0,0,0,0,1,1,1,0,1,1,1,0,0,0,0,1) \xrightarrow{1r} (1,0,0,1,0,1,0,0,1,0,0,0,1,1,1,0)$	5,7,10,16,17,18	6,9,11,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,1,1,0,0,0,1,0) \xrightarrow{1r} (1,0,1,0,1,0,1,0,0,1,1,1,0,0,0,0)$	5,7,10,18	6,9,11,15,18	2^{-23}
$(0,0,0,0,1,1,1,0,1,1,1,0,0,0,1,1) \xrightarrow{1r} (0,1,0,1,0,1,0,1,1,0,0,0,1,1,1,0)$	5,7,10,16,17	6,9,11,15,17	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,1,1,0,0,1,0,0) \xrightarrow{1r} (1,0,1,1,0,1,1,0,0,0,0,0,1,1,1,1)$	5,7,10,14,17,18	6,9,11,17,18	$2^{-6.5}$
$(0,0,0,0,1,1,1,0,1,1,1,0,0,1,0,1) \xrightarrow{1r} (0,1,0,0,1,0,0,1,1,1,1,1,0,0,0,1)$	5,7,10,14,16	6,9,11	2^{-23}
$(0,0,0,0,1,1,1,0,1,1,1,0,0,1,1,0) \xrightarrow{1r} (0,1,1,1,0,1,1,1,0,0,0,0,1,1,1,1)$	5,7,10,14,17	6,9,11,15,17	$2^{-6.5}$
$(0,0,0,0,1,1,1,0,1,1,1,0,0,1,1,1) \xrightarrow{1r} (1,0,0,0,1,0,0,0,1,1,1,1,0,0,0,1)$	5,7,10,14,16,18	6,9,11,15,18	2^{-23}
$(0,0,0,0,1,1,1,0,1,1,1,0,1,0,0,0) \xrightarrow{1r} (1,0,1,1,1,1,1,0,0,1,1,0,0,0,0,0)$	5,7,10,18	6,9,11,13,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,1,1,0,1,0,0,1) \xrightarrow{1r} (0,1,0,0,0,0,0,0,1,1,0,0,1,1,1,0)$	5,7,10,16,17	6,9,11,13,17	2^{-12}
$(0,0,0,0,1,1,1,0,1,1,1,0,1,0,1,0) \xrightarrow{1r} (0,1,1,1,1,1,1,0,0,0,1,1,0,0,0,0)$	5,7,10	6,9,11,13,15	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,1,1,0,1,0,1,1) \xrightarrow{1r} (1,0,0,0,0,0,0,0,1,1,1,0,0,1,1,0)$	5,7,10,16,17,18	6,9,11,13,15,17,18	2^{-12}
$(0,0,0,0,1,1,1,0,1,1,1,0,1,1,0,0) \xrightarrow{1r} (0,1,1,0,0,0,1,0,0,1,0,0,1,1,1,1)$	5,7,10,14,17	6,9,11,13,17	2^{-12}
$(0,0,0,0,1,1,1,0,1,1,1,0,1,1,0,1) \xrightarrow{1r} (1,0,0,1,1,1,0,1,1,0,1,1,0,0,0,1)$	5,7,10,14,16,18	6,9,11,13,18	$2^{-28.5}$
$(0,0,0,0,1,1,1,0,1,1,1,0,1,1,1,0) \xrightarrow{1r} (1,0,1,0,0,0,1,1,0,1,0,0,1,1,1,1)$	5,7,10,14,17,18	6,9,11,13,15,17,18	2^{-12}
$(0,0,0,0,1,1,1,0,1,1,1,0,1,1,1,1) \xrightarrow{1r} (0,1,0,1,1,1,0,0,1,0,1,1,0,0,0,1)$	5,7,10,14,16	6,9,11,13,15	$2^{-28.5}$
$(0,0,0,0,1,1,1,0,1,1,1,1,0,0,0,0) \xrightarrow{1r} (1,0,1,1,0,1,0,0,0,0,1,0,1,1,1,1)$	5,7,10,12,17,18	6,9,11,17,18	$2^{-6.5}$
$(0,0,0,0,1,1,1,0,1,1,1,1,0,0,0,1) \xrightarrow{1r} (0,1,0,0,1,0,1,1,1,1,0,1,0,0,0,1)$	5,7,10,12,16	6,9,11	2^{-12}
$(0,0,0,0,1,1,1,0,1,1,1,1,0,0,1,0) \xrightarrow{1r} (0,1,1,1,0,1,0,1,0,0,1,0,1,1,1,1)$	5,7,10,12,17	6,9,11,15,17	$2^{-6.5}$
$(0,0,0,0,1,1,1,0,1,1,1,1,0,0,1,1) \xrightarrow{1r} (1,0,0,0,1,0,1,0,1,1,0,1,0,0,0,1)$	5,7,10,12,16,18	6,9,11,15,18	2^{-12}
$(0,0,0,0,1,1,1,0,1,1,1,1,0,1,0,0) \xrightarrow{1r} (0,1,1,0,1,0,0,1,0,1,0,1,0,0,0,0)$	5,7,10,12,14	6,9,11	2^{-12}
$(0,0,0,0,1,1,1,0,1,1,1,1,0,1,0,1) \xrightarrow{1r} (1,0,0,1,0,1,1,0,1,0,1,0,1,1,1,0)$	5,7,10,12,14,16,17,18	6,9,11,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,1,1,1,0,1,1,0) \xrightarrow{1r} (1,0,1,0,1,0,0,0,0,1,0,1,0,0,0,0)$	5,7,10,12,14,18	6,9,11,15,18	2^{-12}
$(0,0,0,0,1,1,1,0,1,1,1,1,0,1,1,1) \xrightarrow{1r} (0,1,0,1,0,1,1,1,1,0,1,0,1,1,1,0)$	5,7,10,12,14,16,17	6,9,11,15,17	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,1,1,1,1,0,0,0) \xrightarrow{1r} (0,1,1,0,0,0,0,0,0,1,1,0,1,1,1,1)$	5,7,10,12,17	6,9,11,13,17	2^{-12}
$(0,0,0,0,1,1,1,0,1,1,1,1,1,0,0,1) \xrightarrow{1r} (1,0,0,1,1,1,1,1,1,0,0,1,0,0,0,1)$	5,7,10,12,16,18	6,9,11,13,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,1,1,1,1,0,1,0) \xrightarrow{1r} (1,0,1,0,0,0,0,0,1,0,1,1,0,1,1,1)$	5,7,10,12,17,18	6,9,11,13,15,17,18	2^{-12}
$(0,0,0,0,1,1,1,0,1,1,1,1,1,0,1,1) \xrightarrow{1r} (0,1,0,1,1,1,1,0,1,0,0,1,0,0,0,1)$	5,7,10,12,16	6,9,11,13,15	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,1,1,1,1,1,0,0) \xrightarrow{1r} (1,0,1,1,1,1,0,1,0,0,0,1,0,0,0,0)$	5,7,10,12,14,18	6,9,11,13,18	$2^{-6.5}$
$(0,0,0,0,1,1,1,0,1,1,1,1,1,1,0,1) \xrightarrow{1r} (0,1,0,0,0,0,1,0,1,1,1,0,1,1,1,0)$	5,7,10,12,14,16,17	6,9,11,13,17	2^{-12}
$(0,0,0,0,1,1,1,0,1,1,1,1,1,1,1,0) \xrightarrow{1r} (0,1,1,1,1,1,0,0,0,0,0,1,0,0,0,0)$	5,7,10,12,14	6,9,11,13,15	$2^{-6.5}$
$(0,0,0,0,1,1,1,0,1,1,1,1,1,1,1,1) \xrightarrow{1r} (1,0,0,0,0,0,1,1,1,1,1,0,1,1,1,0)$	5,7,10,12,14,16,17,18	6,9,11,13,15,17,18	2^{-12}

Table 0.121 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	5,7	6,8	$2^{-6.5}$
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	5,7,16,17,18	6,8,17,18	2^{-12}
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	5,7,18	6,8,15,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	5,7,16,17	6,8,15,17	2^{-12}
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	5,7,14,17,18	6,8,17,18	2^{-23}
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	5,7,14,16	6,8	$2^{-6.5}$
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	5,7,14,17	6,8,15,17	2^{-23}
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	5,7,14,16,18	6,8,15,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	5,7,18	6,8,13,18	2^{-12}
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	5,7,16,17	6,8,13,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	5,7	6,8,13,15	2^{-12}
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	5,7,16,17,18	6,8,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	5,7,14,17	6,8,13,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	5,7,14,16,18	6,8,13,18	2^{-1}
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	5,7,14,17,18	6,8,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	5,7,14,16	6,8,13,15	2^{-1}
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	5,7,12,17,18	6,8,17,18	2^{-23}
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	5,7,12,16	6,8	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	5,7,12,17	6,8,15,17	2^{-23}
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	5,7,12,16,18	6,8,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	5,7,12,14	6,8	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	5,7,12,14,16,17,18	6,8,17,18	2^{-12}
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	5,7,12,14,18	6,8,15,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	5,7,12,14,16,17	6,8,15,17	2^{-12}
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	5,7,12,17	6,8,13,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	5,7,12,16,18	6,8,13,18	2^{-12}
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	5,7,12,17,18	6,8,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	5,7,12,16	6,8,13,15	2^{-12}
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	5,7,12,14,18	6,8,13,18	2^{-23}
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	5,7,12,14,16,17	6,8,13,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	5,7,12,14	6,8,13,15	2^{-23}
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	5,7,12,14,16,17,18	6,8,13,15,17,18	$2^{-17.5}$

Table 0.122 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	5,7,18	6,8,11,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	5,7,16,17	6,8,11,17	2^{-23}
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	5,7	6,8,11,15	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	5,7,16,17,18	6,8,11,15,17,18	2^{-23}
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	5,7,14,17	6,8,11,17	2^{-23}
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	5,7,14,16,18	6,8,11,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	5,7,14,17,18	6,8,11,15,17,18	2^{-23}
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	5,7,14,16	6,8,11,15	$2^{-6.5}$
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	5,7	6,8,11,13	2^{-12}
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	5,7,16,17,18	6,8,11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	5,7,18	6,8,11,13,15,18	2^{-12}
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	5,7,16,17	6,8,11,13,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	5,7,14,17,18	6,8,11,13,17,18	$2^{-28.5}$
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	5,7,14,16	6,8,11,13	2^{-12}
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	5,7,14,17	6,8,11,13,15,17	$2^{-28.5}$
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	5,7,14,16,18	6,8,11,13,15,18	2^{-12}
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	5,7,12,17	6,8,11,17	2^{-12}
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	5,7,12,16,18	6,8,11,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	5,7,12,17,18	6,8,11,15,17,18	2^{-12}
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	5,7,12,16	6,8,11,15	$2^{-6.5}$
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	5,7,12,14,18	6,8,11,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	5,7,12,14,16,17	6,8,11,17	2^{-12}
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	5,7,12,14	6,8,11,15	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	5,7,12,14,16,17,18	6,8,11,15,17,18	2^{-12}
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	5,7,12,17,18	6,8,11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	5,7,12,16	6,8,11,13	2^{-12}
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	5,7,12,17	6,8,11,13,15,17	$2^{-17.5}$
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	5,7,12,16,18	6,8,11,13,15,18	2^{-12}
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	5,7,12,14	6,8,11,13	2^{-12}
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	5,7,12,14,16,17,18	6,8,11,13,17,18	$2^{-6.5}$
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	5,7,12,14,18	6,8,11,13,15,18	2^{-12}
$(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	5,7,12,14,16,17	6,8,11,13,15,17	$2^{-6.5}$

Table 0.123 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,1,1,1,0,1,0,0,0,0,0,0) \xrightarrow{1r} (1,1,0,0,0,1,0,1,1,0,0,0,1,0,0,1)$	5,7,10,17,18	6,8,17,18	2^{-23}
$(0,0,0,0,1,1,1,1,0,1,0,0,0,0,0,1) \xrightarrow{1r} (0,0,1,1,1,0,1,0,0,1,1,1,0,1,1,1)$	5,7,10,16	6,8	$2^{-28.5}$
$(0,0,0,0,1,1,1,1,0,1,0,0,0,0,1,0) \xrightarrow{1r} (0,0,0,0,0,1,0,0,1,0,0,0,1,0,0,1)$	5,7,10,17	6,8,15,17	2^{-23}
$(0,0,0,0,1,1,1,1,0,1,0,0,0,0,1,1) \xrightarrow{1r} (1,1,1,1,1,0,1,1,0,1,1,1,0,1,1,1)$	5,7,10,16,18	6,8,15,18	$2^{-28.5}$
$(0,0,0,0,1,1,1,1,0,1,0,0,0,1,0,0) \xrightarrow{1r} (0,0,0,1,1,0,0,0,1,1,1,1,0,1,1,0)$	5,7,10,14	6,8	$2^{-28.5}$
$(0,0,0,0,1,1,1,1,0,1,0,0,0,1,0,1) \xrightarrow{1r} (1,1,1,0,0,1,1,1,0,0,0,0,1,0,0,0)$	5,7,10,14,16,17,18	6,8,17,18	2^{-12}
$(0,0,0,0,1,1,1,1,0,1,0,0,0,1,1,0) \xrightarrow{1r} (1,1,0,1,1,0,0,1,1,1,1,1,0,1,1,0)$	5,7,10,14,18	6,8,15,18	$2^{-28.5}$
$(0,0,0,0,1,1,1,1,0,1,0,0,0,1,1,1) \xrightarrow{1r} (0,0,1,0,0,1,1,0,0,0,0,0,1,0,0,0)$	5,7,10,14,16,17	6,8,15,17	2^{-12}
$(0,0,0,0,1,1,1,1,0,1,0,0,1,0,0,0) \xrightarrow{1r} (0,0,0,1,0,0,0,1,1,1,0,0,1,0,0,1)$	5,7,10,17	6,8,13,17	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,0,1,0,0,1,0,0,1) \xrightarrow{1r} (1,1,1,0,1,1,1,0,0,0,1,1,0,1,1,1)$	5,7,10,16,18	6,8,13,18	2^{-23}
$(0,0,0,0,1,1,1,1,0,1,0,0,1,0,1,0) \xrightarrow{1r} (1,1,0,1,0,0,0,0,1,1,0,0,1,0,0,1)$	5,7,10,17,18	6,8,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,0,1,0,0,1,0,1,1) \xrightarrow{1r} (0,0,1,0,1,1,1,1,0,0,1,1,0,1,1,1)$	5,7,10,16	6,8,13,15	2^{-23}
$(0,0,0,0,1,1,1,1,0,1,0,0,1,1,0,0) \xrightarrow{1r} (1,1,0,0,1,1,0,0,1,0,1,1,0,1,1,0)$	5,7,10,14,18	6,8,13,18	2^{-34}
$(0,0,0,0,1,1,1,1,0,1,0,0,1,1,0,1) \xrightarrow{1r} (0,0,1,1,0,0,1,1,0,1,0,0,1,0,0,0)$	5,7,10,14,16,17	6,8,13,17	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,0,1,0,0,1,1,1,0) \xrightarrow{1r} (0,0,0,0,1,1,0,1,1,0,1,1,0,1,1,0)$	5,7,10,14	6,8,13,15	2^{-34}
$(0,0,0,0,1,1,1,1,0,1,0,0,1,1,1,1) \xrightarrow{1r} (1,1,1,1,0,0,1,0,0,1,0,0,1,0,0,0)$	5,7,10,14,16,17,18	6,8,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,0,1,0,1,0,0,0,0) \xrightarrow{1r} (0,0,0,1,1,0,1,0,1,1,0,1,0,1,1,0)$	5,7,10,12	6,8	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,0,1,0,1,0,0,0,1) \xrightarrow{1r} (1,1,1,0,0,1,0,1,0,0,1,0,1,0,0,0)$	5,7,10,12,16,17,18	6,8,17,18	2^{-12}
$(0,0,0,0,1,1,1,1,0,1,0,1,0,0,1,0) \xrightarrow{1r} (1,1,0,1,1,0,1,1,1,1,0,1,0,1,1,0)$	5,7,10,12,18	6,8,15,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,0,1,0,1,0,0,1,1) \xrightarrow{1r} (0,0,1,0,0,1,0,0,0,0,1,0,1,0,0,0)$	5,7,10,12,16,17	6,8,15,17	2^{-12}
$(0,0,0,0,1,1,1,1,0,1,0,1,0,1,0,0) \xrightarrow{1r} (1,1,0,0,0,1,1,1,1,0,1,0,1,0,0,1)$	5,7,10,12,14,17,18	6,8,17,18	2^{-23}
$(0,0,0,0,1,1,1,1,0,1,0,1,0,1,0,1) \xrightarrow{1r} (0,0,1,1,1,0,0,0,0,1,0,1,0,1,1,1)$	5,7,10,12,14,16	6,8	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,0,1,0,1,0,1,1,0) \xrightarrow{1r} (0,0,0,0,0,1,1,0,1,0,1,0,1,0,0,1)$	5,7,10,12,14,17	6,8,15,17	2^{-23}
$(0,0,0,0,1,1,1,1,0,1,0,1,0,1,1,1) \xrightarrow{1r} (1,1,1,1,1,0,0,1,0,1,0,1,0,1,1,1)$	5,7,10,12,14,16,18	6,8,15,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,0,1,0,1,1,0,0,0) \xrightarrow{1r} (1,1,0,0,1,1,1,0,1,0,0,1,0,1,1,0)$	5,7,10,12,18	6,8,13,18	2^{-23}
$(0,0,0,0,1,1,1,1,0,1,0,1,1,0,0,1) \xrightarrow{1r} (0,0,1,1,0,0,0,1,0,1,1,0,1,0,0,0)$	5,7,10,12,16,17	6,8,13,17	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,0,1,0,1,1,0,1,0) \xrightarrow{1r} (0,0,0,0,1,1,1,1,1,0,0,1,0,1,1,0)$	5,7,10,12	6,8,13,15	2^{-23}
$(0,0,0,0,1,1,1,1,0,1,0,1,1,0,1,1) \xrightarrow{1r} (1,1,1,1,0,0,0,0,0,1,1,0,1,0,0,0)$	5,7,10,12,16,17,18	6,8,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,0,1,0,1,1,1,0,0) \xrightarrow{1r} (0,0,0,1,0,0,1,1,1,1,1,0,1,0,0,1)$	5,7,10,12,14,17	6,8,13,17	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,0,1,0,1,1,1,0,1) \xrightarrow{1r} (1,1,1,0,1,1,0,0,0,0,0,1,0,1,1,1)$	5,7,10,12,14,16,18	6,8,13,18	2^{-12}
$(0,0,0,0,1,1,1,1,0,1,0,1,1,1,1,0) \xrightarrow{1r} (1,1,0,1,0,0,1,0,1,1,1,0,1,0,0,1)$	5,7,10,12,14,17,18	6,8,13,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,0,1,0,1,1,1,1,1) \xrightarrow{1r} (0,0,1,0,1,1,0,1,1,0,0,0,1,0,1,1)$	5,7,10,12,14,16	6,8,13,15	2^{-12}

Table 0.124 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,1,1,0,1,1,0,0,0,0,0) \xrightarrow{1r} (0,0,0,0,0,0,0,1,1,1,0,1,1,0,0,1)$	5,7,10,17	6,8,11,17	2^{-12}
$(0,0,0,0,1,1,1,0,1,1,0,0,0,0,1) \xrightarrow{1r} (1,1,1,1,1,1,1,0,0,0,1,0,0,1,1,1)$	5,7,10,16,18	6,8,11,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,1,0,0,0,1,0) \xrightarrow{1r} (1,1,0,0,0,0,0,0,1,1,0,1,1,0,0,1)$	5,7,10,17,18	6,8,11,15,17,18	2^{-12}
$(0,0,0,0,1,1,1,0,1,1,0,0,0,1,1) \xrightarrow{1r} (0,0,1,1,1,1,1,1,0,0,1,0,0,1,1,1)$	5,7,10,16	6,8,11,15	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,1,0,0,1,0,0) \xrightarrow{1r} (1,1,0,1,1,1,0,0,1,0,1,0,0,1,1,0)$	5,7,10,14,18	6,8,11,18	$2^{-28.5}$
$(0,0,0,0,1,1,1,0,1,1,0,0,1,0,1) \xrightarrow{1r} (0,0,1,0,0,0,1,1,0,1,0,1,1,0,0,0)$	5,7,10,14,16,17	6,8,11,17	2^{-12}
$(0,0,0,0,1,1,1,0,1,1,0,0,1,1,0) \xrightarrow{1r} (0,0,0,1,1,1,0,1,1,0,1,0,0,1,1,0)$	5,7,10,14	6,8,11,15	$2^{-28.5}$
$(0,0,0,0,1,1,1,0,1,1,0,0,1,1,1) \xrightarrow{1r} (1,1,1,0,0,0,1,0,0,1,0,1,1,0,0,0)$	5,7,10,14,16,17,18	6,8,11,15,17,18	2^{-12}
$(0,0,0,0,1,1,1,0,1,1,0,1,0,0,0) \xrightarrow{1r} (1,1,0,1,0,1,0,1,1,0,0,1,1,0,0,1)$	5,7,10,17,18	6,8,11,13,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,1,0,1,0,0,1) \xrightarrow{1r} (0,0,1,0,1,0,1,0,0,1,1,0,0,1,1,1)$	5,7,10,16	6,8,11,13	2^{-23}
$(0,0,0,0,1,1,1,0,1,1,0,1,0,1,0) \xrightarrow{1r} (0,0,0,1,0,1,0,0,1,0,0,1,1,0,0,1)$	5,7,10,17	6,8,11,13,15,17	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,1,0,1,0,1,1) \xrightarrow{1r} (1,1,1,0,1,0,1,1,0,1,1,0,0,1,1,1)$	5,7,10,16,18	6,8,11,13,15,18	2^{-23}
$(0,0,0,0,1,1,1,0,1,1,0,1,1,0,0) \xrightarrow{1r} (0,0,0,0,1,0,0,0,1,1,1,0,0,1,1,0)$	5,7,10,14	6,8,11,13	2^{-23}
$(0,0,0,0,1,1,1,0,1,1,0,1,1,0,1) \xrightarrow{1r} (1,1,1,1,0,1,1,1,0,0,0,1,1,0,0,0)$	5,7,10,14,16,17,18	6,8,11,13,17,18	$2^{-6.5}$
$(0,0,0,0,1,1,1,0,1,1,0,1,1,1,0) \xrightarrow{1r} (1,1,0,0,1,0,0,1,1,1,1,0,0,1,1,0)$	5,7,10,14,18	6,8,11,13,15,18	2^{-23}
$(0,0,0,0,1,1,1,0,1,1,0,1,1,1,1) \xrightarrow{1r} (0,0,1,1,0,1,1,0,0,0,0,1,1,0,0,0)$	5,7,10,14,16,17	6,8,11,13,15,17	$2^{-6.5}$
$(0,0,0,0,1,1,1,0,1,1,1,0,0,0,0) \xrightarrow{1r} (1,1,0,1,1,1,1,0,1,0,0,0,0,1,1,0)$	5,7,10,12,18	6,8,11,18	$2^{-28.5}$
$(0,0,0,0,1,1,1,0,1,1,1,0,0,0,1) \xrightarrow{1r} (0,0,1,0,0,0,0,1,0,1,1,1,1,0,0,0)$	5,7,10,12,16,17	6,8,11,17	2^{-23}
$(0,0,0,0,1,1,1,0,1,1,1,0,0,1,0) \xrightarrow{1r} (0,0,0,1,1,1,1,1,1,0,0,0,0,1,1,0)$	5,7,10,12	6,8,11,15	$2^{-28.5}$
$(0,0,0,0,1,1,1,0,1,1,1,0,0,1,1) \xrightarrow{1r} (1,1,1,0,0,0,0,0,0,1,1,1,1,0,0,0)$	5,7,10,12,16,17,18	6,8,11,15,17,18	2^{-23}
$(0,0,0,0,1,1,1,0,1,1,1,0,1,0,0) \xrightarrow{1r} (0,0,0,0,0,0,1,1,1,1,1,1,0,0,1)$	5,7,10,12,14,17	6,8,11,17	2^{-23}
$(0,0,0,0,1,1,1,0,1,1,1,0,1,0,1) \xrightarrow{1r} (1,1,1,1,1,1,0,0,0,0,0,0,1,1,1)$	5,7,10,12,14,16,18	6,8,11,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,1,1,0,1,1,0) \xrightarrow{1r} (1,1,0,0,0,0,1,0,1,1,1,1,1,0,0,1)$	5,7,10,12,14,17,18	6,8,11,15,17,18	2^{-23}
$(0,0,0,0,1,1,1,0,1,1,1,0,1,1,1) \xrightarrow{1r} (0,0,1,1,1,1,0,1,0,0,0,0,0,1,1,1)$	5,7,10,12,14,16	6,8,11,15	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,1,1,1,0,0,0) \xrightarrow{1r} (0,0,0,0,1,0,1,0,1,1,1,0,0,0,1,1,0)$	5,7,10,12	6,8,11,13	2^{-23}
$(0,0,0,0,1,1,1,0,1,1,1,1,0,0,1) \xrightarrow{1r} (1,1,1,1,0,1,0,1,0,1,0,0,1,1,1,0,0,0)$	5,7,10,12,16,17,18	6,8,11,13,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,1,1,1,0,1,0) \xrightarrow{1r} (1,1,0,0,1,0,1,1,1,1,0,0,0,1,1,0)$	5,7,10,12,18	6,8,11,13,15,18	2^{-23}
$(0,0,0,0,1,1,1,0,1,1,1,1,0,1,1) \xrightarrow{1r} (0,0,1,1,0,1,0,0,0,0,1,1,1,0,0,0)$	5,7,10,12,16,17	6,8,11,13,15,17	$2^{-17.5}$
$(0,0,0,0,1,1,1,0,1,1,1,1,1,0,0) \xrightarrow{1r} (1,1,0,1,0,1,1,1,1,0,1,1,1,0,0,1)$	5,7,10,12,14,17,18	6,8,11,13,17,18	$2^{-28.5}$
$(0,0,0,0,1,1,1,0,1,1,1,1,1,0,1) \xrightarrow{1r} (0,0,1,0,1,0,0,0,0,1,0,0,0,1,1,1)$	5,7,10,12,14,16	6,8,11,13	2^{-23}
$(0,0,0,0,1,1,1,0,1,1,1,1,1,1,0) \xrightarrow{1r} (0,0,0,1,0,1,1,0,1,0,1,0,1,1,1,0,0,1)$	5,7,10,12,14,17	6,8,11,13,15,17	$2^{-28.5}$
$(0,0,0,0,1,1,1,0,1,1,1,1,1,1,1) \xrightarrow{1r} (1,1,1,0,1,0,0,1,0,1,0,0,0,1,1,1)$	5,7,10,12,14,16,18	6,8,11,13,15,18	2^{-23}

Table 0.125 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,1,1,1,1,0,0,0,0,0,0,0) \xrightarrow{1r} (1,0,1,0,0,1,0,1,1,0,0,0,1,0,1,0)$	5,7,18	6,8,9,18	2^{-23}
$(0,0,0,0,1,1,1,1,1,0,0,0,0,0,0,1) \xrightarrow{1r} (0,1,0,1,1,0,1,0,0,1,1,1,0,1,0,0)$	5,7,16,17	6,8,9,17	$2^{-28.5}$
$(0,0,0,0,1,1,1,1,1,0,0,0,0,0,1,0) \xrightarrow{1r} (0,1,1,0,0,1,0,0,1,0,0,0,1,0,1,0)$	5,7	6,8,9,15	2^{-23}
$(0,0,0,0,1,1,1,1,1,0,0,0,0,0,1,1) \xrightarrow{1r} (1,0,0,1,1,0,1,1,0,1,1,1,0,1,0,0)$	5,7,16,17,18	6,8,9,15,17,18	$2^{-28.5}$
$(0,0,0,0,1,1,1,1,1,0,0,0,0,1,0,0) \xrightarrow{1r} (0,1,1,1,1,0,0,0,1,1,1,1,0,1,0,1)$	5,7,14,17	6,8,9,17	$2^{-28.5}$
$(0,0,0,0,1,1,1,1,1,0,0,0,0,1,0,1) \xrightarrow{1r} (1,0,0,0,0,1,1,1,0,0,0,0,1,0,1,1)$	5,7,14,16,18	6,8,9,18	2^{-12}
$(0,0,0,0,1,1,1,1,1,0,0,0,0,1,1,0) \xrightarrow{1r} (1,0,1,1,1,0,0,1,1,1,1,1,0,1,0,1)$	5,7,14,17,18	6,8,9,15,17,18	$2^{-28.5}$
$(0,0,0,0,1,1,1,1,1,0,0,0,0,1,1,1) \xrightarrow{1r} (0,1,0,0,0,1,1,0,0,0,0,0,1,0,1,1)$	5,7,14,16	6,8,9,15	2^{-12}
$(0,0,0,0,1,1,1,1,1,0,0,0,1,0,0,0) \xrightarrow{1r} (0,1,1,1,0,0,0,1,1,1,0,0,1,0,1,0)$	5,7	6,8,9,13	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,0,0,0,1,0,0,1) \xrightarrow{1r} (1,0,0,0,1,1,1,0,0,0,1,1,0,1,0,0)$	5,7,16,17,18	6,8,9,13,17,18	2^{-23}
$(0,0,0,0,1,1,1,1,1,0,0,0,1,0,1,0) \xrightarrow{1r} (1,0,1,1,0,0,0,0,1,1,0,0,1,0,1,0)$	5,7,18	6,8,9,13,15,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,0,0,0,1,0,1,1) \xrightarrow{1r} (0,1,0,0,1,1,1,1,0,0,1,1,0,1,0,0)$	5,7,16,17	6,8,9,13,15,17	2^{-23}
$(0,0,0,0,1,1,1,1,1,0,0,0,1,1,0,0) \xrightarrow{1r} (1,0,1,0,1,1,0,0,1,0,1,1,0,1,0,1)$	5,7,14,17,18	6,8,9,13,17,18	2^{-34}
$(0,0,0,0,1,1,1,1,1,0,0,0,1,1,0,1) \xrightarrow{1r} (0,1,0,1,0,0,1,1,0,1,0,0,1,0,1,1)$	5,7,14,16	6,8,9,13	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,0,0,0,1,1,0,1) \xrightarrow{1r} (0,1,1,0,1,1,0,1,1,0,1,1,0,1,0,1)$	5,7,14,17	6,8,9,13,15,17	2^{-34}
$(0,0,0,0,1,1,1,1,1,0,0,0,1,1,1,0) \xrightarrow{1r} (1,0,0,1,0,0,1,0,0,1,0,0,1,0,1,1)$	5,7,14,16,18	6,8,9,13,15,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,0,0,0,1,0,0,0) \xrightarrow{1r} (0,1,1,1,1,0,1,0,1,1,0,1,0,1,0,1)$	5,7,12,17	6,8,9,17	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,0,0,0,1,0,0,1) \xrightarrow{1r} (1,0,0,0,0,1,0,1,0,0,1,0,1,0,1,1)$	5,7,12,16,18	6,8,9,18	2^{-12}
$(0,0,0,0,1,1,1,1,1,0,0,0,1,0,1,0) \xrightarrow{1r} (1,0,1,1,1,0,1,1,1,1,0,1,0,1,0,1)$	5,7,12,17,18	6,8,9,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,0,0,0,1,0,1,1) \xrightarrow{1r} (0,1,0,0,0,1,0,0,0,0,1,0,1,0,1,1)$	5,7,12,16	6,8,9,15	2^{-12}
$(0,0,0,0,1,1,1,1,1,0,0,0,1,0,1,0) \xrightarrow{1r} (1,0,1,0,0,1,1,1,1,0,1,0,1,0,1,0)$	5,7,12,14,18	6,8,9,18	2^{-23}
$(0,0,0,0,1,1,1,1,1,0,0,0,1,0,1,0) \xrightarrow{1r} (0,1,0,1,1,0,0,0,0,1,0,1,0,1,0,0)$	5,7,12,14,16,17	6,8,9,17	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,0,0,0,1,0,1,1) \xrightarrow{1r} (0,1,1,0,0,1,1,0,1,0,1,0,1,0,1,0)$	5,7,12,14	6,8,9,15	2^{-23}
$(0,0,0,0,1,1,1,1,1,0,0,0,1,0,1,1) \xrightarrow{1r} (1,0,0,1,1,0,0,1,0,1,0,1,0,1,0,0)$	5,7,12,14,16,17,18	6,8,9,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,0,0,0,1,0,0,0) \xrightarrow{1r} (1,0,1,0,1,1,1,0,1,0,0,1,0,1,0,1)$	5,7,12,17,18	6,8,9,13,17,18	2^{-23}
$(0,0,0,0,1,1,1,1,1,0,0,0,1,0,0,1) \xrightarrow{1r} (0,1,0,1,0,0,0,1,0,1,1,0,1,0,1,1)$	5,7,12,16	6,8,9,13	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,0,0,0,1,0,1,0) \xrightarrow{1r} (0,1,1,0,1,1,1,1,0,0,1,0,1,0,1,0)$	5,7,12,17	6,8,9,13,15,17	2^{-23}
$(0,0,0,0,1,1,1,1,1,0,0,0,1,0,1,1) \xrightarrow{1r} (1,0,0,1,0,0,0,0,0,1,1,0,1,0,1,1)$	5,7,12,16,18	6,8,9,13,15,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,0,0,0,1,1,0,0) \xrightarrow{1r} (0,1,1,1,0,0,1,1,1,1,1,0,1,0,1,0)$	5,7,12,14	6,8,9,13	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,0,0,0,1,1,0,1) \xrightarrow{1r} (1,0,0,0,1,1,0,0,0,0,0,1,0,1,0,0)$	5,7,12,14,16,17,18	6,8,9,13,17,18	2^{-12}
$(0,0,0,0,1,1,1,1,1,0,0,0,1,1,1,0) \xrightarrow{1r} (1,0,1,1,0,0,1,0,1,1,1,0,1,0,1,0)$	5,7,12,14,18	6,8,9,13,15,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,0,0,0,1,1,1,1) \xrightarrow{1r} (0,1,0,0,1,1,0,1,0,0,0,1,0,1,0,0)$	5,7,12,14,16,17	6,8,9,13,15,17	2^{-12}

Table 0.126 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,1,1,1,1,0,1,0,0,0,0,0) \xrightarrow{1r} (0,1,1,0,0,0,0,1,1,1,0,1,1,0,1,0)$	5,7	6,8,9,11	2^{-12}
$(0,0,0,0,1,1,1,1,1,0,1,0,0,0,0,1) \xrightarrow{1r} (1,0,0,1,1,1,1,0,0,0,1,0,0,1,0,0)$	5,7,16,17,18	6,8,9,11,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,0,1,0,0,0,1,0) \xrightarrow{1r} (1,0,1,0,0,0,0,0,1,1,0,1,1,0,1,0)$	5,7,18	6,8,9,11,15,18	2^{-12}
$(0,0,0,0,1,1,1,1,1,0,1,0,0,0,1,1) \xrightarrow{1r} (0,1,0,1,1,1,1,1,0,0,1,0,0,1,0,0)$	5,7,16,17	6,8,9,11,15,17	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,0,1,0,0,1,0,0) \xrightarrow{1r} (1,0,1,1,1,1,0,0,1,0,1,0,0,1,0,1)$	5,7,14,17,18	6,8,9,11,17,18	$2^{-28.5}$
$(0,0,0,0,1,1,1,1,1,0,1,0,0,1,0,1) \xrightarrow{1r} (0,1,0,0,0,0,1,1,0,1,0,1,1,0,1,1)$	5,7,14,16	6,8,9,11	2^{-12}
$(0,0,0,0,1,1,1,1,1,0,1,0,0,1,1,0) \xrightarrow{1r} (0,1,1,1,1,1,0,1,1,0,1,0,0,1,0,1)$	5,7,14,17	6,8,9,11,15,17	$2^{-28.5}$
$(0,0,0,0,1,1,1,1,1,0,1,0,0,1,1,1) \xrightarrow{1r} (1,0,0,0,0,0,1,0,0,1,0,1,1,0,1,1)$	5,7,14,16,18	6,8,9,11,15,18	2^{-12}
$(0,0,0,0,1,1,1,1,1,0,1,0,0,0,0,0) \xrightarrow{1r} (1,0,1,1,0,1,0,1,1,0,0,1,1,0,1,0)$	5,7,18	6,8,9,11,13,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,0,1,0,0,0,1,0) \xrightarrow{1r} (0,1,0,0,1,0,1,0,0,1,1,0,0,1,0,0)$	5,7,16,17	6,8,9,11,13,17	2^{-23}
$(0,0,0,0,1,1,1,1,1,0,1,0,0,1,0,1) \xrightarrow{1r} (0,1,1,1,0,1,0,0,1,0,0,1,1,0,1,0)$	5,7	6,8,9,11,13,15	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,0,1,0,0,1,0,1) \xrightarrow{1r} (1,0,0,0,1,0,1,1,0,1,1,0,0,1,0,0)$	5,7,16,17,18	6,8,9,11,13,15,17,18	2^{-23}
$(0,0,0,0,1,1,1,1,1,0,1,0,1,1,0,0) \xrightarrow{1r} (0,1,1,0,1,0,0,0,1,1,1,0,0,1,0,1)$	5,7,14,17	6,8,9,11,13,17	2^{-23}
$(0,0,0,0,1,1,1,1,1,0,1,0,1,1,0,1) \xrightarrow{1r} (1,0,0,1,0,1,1,1,0,0,0,1,1,0,1,1)$	5,7,14,16,18	6,8,9,11,13,18	$2^{-6.5}$
$(0,0,0,0,1,1,1,1,1,0,1,0,1,1,1,0) \xrightarrow{1r} (1,0,1,0,1,0,0,1,1,1,1,0,0,1,0,1)$	5,7,14,17,18	6,8,9,11,13,15,17,18	2^{-23}
$(0,0,0,0,1,1,1,1,1,0,1,0,1,1,1,1) \xrightarrow{1r} (0,1,0,1,0,1,1,0,0,0,0,1,1,0,1,1)$	5,7,14,16	6,8,9,11,13,15	$2^{-6.5}$
$(0,0,0,0,1,1,1,1,1,0,1,1,0,0,0,0) \xrightarrow{1r} (1,0,1,1,1,1,1,0,1,0,0,0,0,1,0,1)$	5,7,12,17,18	6,8,9,11,17,18	$2^{-28.5}$
$(0,0,0,0,1,1,1,1,1,0,1,1,0,0,0,1) \xrightarrow{1r} (0,1,0,0,0,0,0,1,0,1,1,1,1,0,1,1)$	5,7,12,16	6,8,9,11	2^{-23}
$(0,0,0,0,1,1,1,1,1,0,1,1,0,0,1,0) \xrightarrow{1r} (0,1,1,1,1,1,1,1,0,0,0,0,1,0,1)$	5,7,12,17	6,8,9,11,15,17	$2^{-28.5}$
$(0,0,0,0,1,1,1,1,1,0,1,1,0,0,1,1) \xrightarrow{1r} (1,0,0,0,0,0,0,0,0,1,1,1,1,0,1,1)$	5,7,12,16,18	6,8,9,11,15,18	2^{-23}
$(0,0,0,0,1,1,1,1,1,0,1,1,0,1,0,0) \xrightarrow{1r} (0,1,1,0,0,0,1,1,1,1,1,1,1,0,1,0)$	5,7,12,14	6,8,9,11	2^{-23}
$(0,0,0,0,1,1,1,1,1,0,1,1,0,1,0,1) \xrightarrow{1r} (1,0,0,1,1,1,0,0,0,0,0,0,0,1,0,0)$	5,7,12,14,16,17,18	6,8,9,11,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,0,1,1,0,1,1,0) \xrightarrow{1r} (1,0,1,0,0,0,1,0,1,1,1,1,1,1,0,1,0)$	5,7,12,14,18	6,8,9,11,15,18	2^{-23}
$(0,0,0,0,1,1,1,1,1,0,1,1,0,1,1,1) \xrightarrow{1r} (0,1,0,1,1,1,0,1,0,0,0,0,0,1,0,0)$	5,7,12,14,16,17	6,8,9,11,15,17	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,0,1,1,0,1,0,0) \xrightarrow{1r} (0,1,1,0,1,0,1,0,1,1,1,0,0,0,1,0,1)$	5,7,12,17	6,8,9,11,13,17	2^{-23}
$(0,0,0,0,1,1,1,1,1,0,1,1,0,0,0,1) \xrightarrow{1r} (1,0,0,1,0,1,0,1,0,0,0,1,1,1,0,1,1)$	5,7,12,16,18	6,8,9,11,13,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,0,1,1,0,1,0,1) \xrightarrow{1r} (1,0,1,0,1,0,1,1,1,1,1,0,0,0,1,0,1)$	5,7,12,17,18	6,8,9,11,13,15,17,18	2^{-23}
$(0,0,0,0,1,1,1,1,1,0,1,1,0,1,1,1) \xrightarrow{1r} (0,1,0,1,0,1,0,0,0,0,0,1,1,1,0,1,1)$	5,7,12,16	6,8,9,11,13,15	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,0,1,1,1,1,0,0) \xrightarrow{1r} (1,0,1,1,0,1,1,1,1,0,1,1,1,0,1,0)$	5,7,12,14,18	6,8,9,11,13,18	$2^{-28.5}$
$(0,0,0,0,1,1,1,1,1,0,1,1,1,1,0,1) \xrightarrow{1r} (0,1,0,0,1,0,0,0,0,1,0,0,0,1,0,0)$	5,7,12,14,16,17	6,8,9,11,13,17	2^{-23}
$(0,0,0,0,1,1,1,1,1,0,1,1,1,1,0,1) \xrightarrow{1r} (0,1,1,1,0,1,1,0,1,0,1,0,1,1,0,1,0)$	5,7,12,14	6,8,9,11,13,15	$2^{-28.5}$
$(0,0,0,0,1,1,1,1,1,0,1,1,1,1,1,1) \xrightarrow{1r} (1,0,0,0,1,0,0,1,0,1,0,1,0,0,0,1,0,0)$	5,7,12,14,16,17,18	6,8,9,11,13,15,17,18	2^{-23}

Table 0.127 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,1,1,1,1,0,0,0,0,0,0) \xrightarrow{1r} (0,1,0,1,0,0,0,0,1,1,0,1,1,1,0,1)$	5,7,10,17	6,8,9,17	$2^{-6.5}$
$(0,0,0,0,1,1,1,1,1,0,0,0,0,0,1) \xrightarrow{1r} (1,0,1,0,1,1,1,1,0,0,1,0,0,0,1,1)$	5,7,10,16,18	6,8,9,18	2^{-12}
$(0,0,0,0,1,1,1,1,1,0,0,0,0,1,0) \xrightarrow{1r} (1,0,0,1,0,0,0,0,1,1,1,0,1,1,1,0,1)$	5,7,10,17,18	6,8,9,15,17,18	$2^{-6.5}$
$(0,0,0,0,1,1,1,1,1,0,0,0,0,1,1) \xrightarrow{1r} (0,1,1,0,1,1,1,0,0,0,1,0,0,0,1,1)$	5,7,10,16	6,8,9,15	2^{-12}
$(0,0,0,0,1,1,1,1,1,0,0,0,1,0,0) \xrightarrow{1r} (1,0,0,0,1,1,0,1,1,0,1,0,0,0,1,0)$	5,7,10,14,18	6,8,9,18	2^{-23}
$(0,0,0,0,1,1,1,1,1,0,0,0,1,0,1) \xrightarrow{1r} (0,1,1,1,0,0,1,0,0,1,0,1,1,1,0,0)$	5,7,10,14,16,17	6,8,9,17	$2^{-6.5}$
$(0,0,0,0,1,1,1,1,1,0,0,0,1,1,0) \xrightarrow{1r} (0,1,0,0,1,1,0,0,1,0,1,0,0,0,1,0)$	5,7,10,14	6,8,9,15	2^{-23}
$(0,0,0,0,1,1,1,1,1,0,0,0,1,1,1) \xrightarrow{1r} (1,0,1,1,0,0,1,1,0,1,0,1,1,1,0,0)$	5,7,10,14,16,17,18	6,8,9,15,17,18	$2^{-6.5}$
$(0,0,0,0,1,1,1,1,1,0,0,1,0,0,0) \xrightarrow{1r} (1,0,0,0,0,1,0,0,1,0,0,1,1,1,0,1)$	5,7,10,17,18	6,8,9,13,17,18	2^{-12}
$(0,0,0,0,1,1,1,1,1,0,0,1,0,0,1) \xrightarrow{1r} (0,1,1,1,0,1,1,0,1,1,0,0,0,1,1)$	5,7,10,16	6,8,9,13	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,0,0,1,0,1,0) \xrightarrow{1r} (0,1,0,0,0,1,0,1,1,0,0,1,1,1,0,1)$	5,7,10,17	6,8,9,13,15,17	2^{-12}
$(0,0,0,0,1,1,1,1,1,0,0,1,0,1,1) \xrightarrow{1r} (1,0,1,1,1,0,1,0,0,1,1,0,0,0,1,1)$	5,7,10,16,18	6,8,9,13,15,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,0,0,1,1,0,0) \xrightarrow{1r} (0,1,0,1,1,0,0,1,1,1,1,0,0,0,1,0)$	5,7,10,14	6,8,9,13	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,0,0,1,1,0,1) \xrightarrow{1r} (1,0,1,0,0,1,1,0,0,0,0,1,1,1,0,0)$	5,7,10,14,16,17,18	6,8,9,13,17,18	2^{-1}
$(0,0,0,0,1,1,1,1,1,0,0,1,1,1,0) \xrightarrow{1r} (1,0,0,1,1,0,0,0,1,1,1,0,0,0,1,0)$	5,7,10,14,18	6,8,9,13,15,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,0,0,1,1,1,1) \xrightarrow{1r} (0,1,1,0,0,1,1,1,0,0,0,1,1,1,0,0)$	5,7,10,14,16,17	6,8,9,13,15,17	2^{-1}
$(0,0,0,0,1,1,1,1,1,0,1,0,0,0,0) \xrightarrow{1r} (1,0,0,0,1,1,1,1,0,0,0,0,0,1,0)$	5,7,10,12,18	6,8,9,18	2^{-23}
$(0,0,0,0,1,1,1,1,1,0,1,0,0,0,1) \xrightarrow{1r} (0,1,1,1,0,0,0,0,0,1,1,1,1,1,0,0)$	5,7,10,12,16,17	6,8,9,17	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,0,1,0,0,1,0) \xrightarrow{1r} (0,1,0,0,1,1,1,0,1,0,0,0,0,0,1,0)$	5,7,10,12	6,8,9,15	2^{-23}
$(0,0,0,0,1,1,1,1,1,0,1,0,0,1,1) \xrightarrow{1r} (1,0,1,1,0,0,0,1,0,1,1,1,1,1,0,0)$	5,7,10,12,16,17,18	6,8,9,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,0,1,0,1,0,0) \xrightarrow{1r} (0,1,0,1,0,0,1,0,1,1,1,1,1,1,0,1)$	5,7,10,12,14,17	6,8,9,17	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,0,1,0,1,0,1) \xrightarrow{1r} (1,0,1,0,1,1,0,1,0,0,0,0,0,0,1,1)$	5,7,10,12,14,16,18	6,8,9,18	2^{-12}
$(0,0,0,0,1,1,1,1,1,0,1,0,1,1,0) \xrightarrow{1r} (1,0,0,1,0,0,1,1,1,1,1,1,1,1,0,1)$	5,7,10,12,14,17,18	6,8,9,15,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,0,1,0,1,1,1) \xrightarrow{1r} (0,1,1,0,1,1,0,0,0,0,0,0,0,0,1,1)$	5,7,10,12,14,16	6,8,9,15	2^{-12}
$(0,0,0,0,1,1,1,1,1,0,1,0,1,1,0,0) \xrightarrow{1r} (0,1,0,1,1,0,1,1,1,1,0,0,0,0,1,0)$	5,7,10,12	6,8,9,13	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,0,1,0,1,1,0,0) \xrightarrow{1r} (1,0,1,0,0,1,0,0,0,0,1,1,1,1,0,0)$	5,7,10,12,16,17,18	6,8,9,13,17,18	2^{-12}
$(0,0,0,0,1,1,1,1,1,0,1,0,1,0,1,0) \xrightarrow{1r} (1,0,0,1,1,0,1,0,1,1,0,0,0,0,1,0)$	5,7,10,12,18	6,8,9,13,15,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,0,1,0,1,0,1,1) \xrightarrow{1r} (0,1,1,0,0,1,0,1,0,0,1,1,1,1,0,0)$	5,7,10,12,16,17	6,8,9,13,15,17	2^{-12}
$(0,0,0,0,1,1,1,1,1,0,1,0,1,1,0,0) \xrightarrow{1r} (1,0,0,0,0,1,1,0,1,0,1,1,1,1,0,1)$	5,7,10,12,14,17,18	6,8,9,13,17,18	2^{-23}
$(0,0,0,0,1,1,1,1,1,0,1,0,1,1,0,1) \xrightarrow{1r} (0,1,1,1,1,0,0,1,0,1,0,0,0,0,1,1)$	5,7,10,12,14,16	6,8,9,13	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,0,1,0,1,1,1,0) \xrightarrow{1r} (0,1,0,0,0,1,1,1,1,0,1,1,1,1,0,1)$	5,7,10,12,14,17	6,8,9,13,15,17	2^{-23}
$(0,0,0,0,1,1,1,1,1,0,1,0,1,1,1,1) \xrightarrow{1r} (1,0,1,1,1,0,0,0,0,1,0,0,0,0,1,1)$	5,7,10,12,14,16,18	6,8,9,13,15,18	$2^{-17.5}$

Table 0.128 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,0,1,1,1,1,1,1,0,0,0,0,0) \xrightarrow{1r} (1,0,0,1,0,1,0,0,1,0,0,0,1,1,0,1)$	5,7,10,17,18	6,8,9,11,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,1,0,0,0,0,1) \xrightarrow{1r} (0,1,1,0,1,0,1,1,0,1,1,1,0,0,1,1)$	5,7,10,16	6,8,9,11	2^{-23}
$(0,0,0,0,1,1,1,1,1,1,0,0,0,1,0) \xrightarrow{1r} (0,1,0,1,0,1,0,1,1,0,0,0,1,1,0,1)$	5,7,10,17	6,8,9,11,15,17	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,1,0,0,0,1,1) \xrightarrow{1r} (1,0,1,0,1,0,1,0,0,1,1,1,0,0,1,1)$	5,7,10,16,18	6,8,9,11,15,18	2^{-23}
$(0,0,0,0,1,1,1,1,1,1,0,0,1,0,0) \xrightarrow{1r} (0,1,0,0,1,0,0,1,1,1,1,1,0,0,1,0)$	5,7,10,14	6,8,9,11	2^{-23}
$(0,0,0,0,1,1,1,1,1,1,0,0,1,0,1) \xrightarrow{1r} (1,0,1,1,0,1,1,0,0,0,0,0,1,1,0,0)$	5,7,10,14,16,17,18	6,8,9,11,17,18	$2^{-6.5}$
$(0,0,0,0,1,1,1,1,1,1,0,0,1,1,0) \xrightarrow{1r} (1,0,0,0,1,0,0,0,1,1,1,1,0,0,1,0)$	5,7,10,14,18	6,8,9,11,15,18	2^{-23}
$(0,0,0,0,1,1,1,1,1,1,0,0,1,1,1) \xrightarrow{1r} (0,1,1,1,0,1,1,1,0,0,0,0,1,1,0,0)$	5,7,10,14,16,17	6,8,9,11,15,17	$2^{-6.5}$
$(0,0,0,0,1,1,1,1,1,1,0,1,0,0,0) \xrightarrow{1r} (0,1,0,0,0,0,0,0,1,1,0,0,1,1,0,1)$	5,7,10,17	6,8,9,11,13,17	2^{-12}
$(0,0,0,0,1,1,1,1,1,1,0,1,0,0,1) \xrightarrow{1r} (1,0,1,1,1,1,1,1,0,0,1,1,0,0,1,1)$	5,7,10,16,18	6,8,9,11,13,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,1,0,1,0,1,0) \xrightarrow{1r} (1,0,0,0,0,0,0,0,1,1,1,0,0,1,1,0,1)$	5,7,10,17,18	6,8,9,11,13,15,17,18	2^{-12}
$(0,0,0,0,1,1,1,1,1,1,0,1,0,1,1) \xrightarrow{1r} (0,1,1,1,1,1,1,1,0,0,0,1,1,0,0,1,1)$	5,7,10,16	6,8,9,11,13,15	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,1,0,1,1,0,0) \xrightarrow{1r} (1,0,0,1,1,1,0,1,1,0,1,1,0,0,1,0)$	5,7,10,14,18	6,8,9,11,13,18	$2^{-28.5}$
$(0,0,0,0,1,1,1,1,1,1,0,1,1,0,1) \xrightarrow{1r} (0,1,1,0,0,0,1,0,0,1,0,0,1,1,0,0)$	5,7,10,14,16,17	6,8,9,11,13,17	2^{-12}
$(0,0,0,0,1,1,1,1,1,1,0,1,1,1,0) \xrightarrow{1r} (0,1,0,1,1,1,0,0,1,0,1,1,0,0,1,0)$	5,7,10,14	6,8,9,11,13,15	$2^{-28.5}$
$(0,0,0,0,1,1,1,1,1,1,0,1,1,1,1) \xrightarrow{1r} (1,0,1,0,0,0,1,1,0,1,0,0,1,1,0,0)$	5,7,10,14,16,17,18	6,8,9,11,13,15,17,18	2^{-12}
$(0,0,0,0,1,1,1,1,1,1,0,0,0,0,0) \xrightarrow{1r} (0,1,0,0,1,0,1,1,1,1,0,0,1,0,0,1,0)$	5,7,10,12	6,8,9,11	2^{-12}
$(0,0,0,0,1,1,1,1,1,1,0,0,0,1,0) \xrightarrow{1r} (1,0,1,1,0,1,0,0,0,0,1,0,1,1,0,0)$	5,7,10,12,16,17,18	6,8,9,11,17,18	$2^{-6.5}$
$(0,0,0,0,1,1,1,1,1,1,0,0,1,0,0) \xrightarrow{1r} (1,0,0,0,1,0,1,0,1,1,0,1,0,0,1,0)$	5,7,10,12,18	6,8,9,11,15,18	2^{-12}
$(0,0,0,0,1,1,1,1,1,1,0,0,1,1,0) \xrightarrow{1r} (0,1,1,1,0,1,0,1,0,0,1,0,1,1,0,0)$	5,7,10,12,16,17	6,8,9,11,15,17	$2^{-6.5}$
$(0,0,0,0,1,1,1,1,1,1,0,0,1,0,0) \xrightarrow{1r} (1,0,0,1,0,1,1,0,1,0,1,0,1,1,0,1)$	5,7,10,12,14,17,18	6,8,9,11,17,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,1,0,0,1,0,1) \xrightarrow{1r} (0,1,1,0,1,0,0,1,0,1,0,1,0,0,1,1)$	5,7,10,12,14,16	6,8,9,11	2^{-12}
$(0,0,0,0,1,1,1,1,1,1,0,0,1,1,0) \xrightarrow{1r} (0,1,0,1,0,1,1,1,1,0,1,0,1,0,1,1,0,1)$	5,7,10,12,14,17	6,8,9,11,15,17	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,1,0,0,1,1,1) \xrightarrow{1r} (1,0,1,0,1,0,0,0,0,0,1,0,1,0,0,1,1)$	5,7,10,12,14,16,18	6,8,9,11,15,18	2^{-12}
$(0,0,0,0,1,1,1,1,1,1,0,0,0,0,0) \xrightarrow{1r} (1,0,0,1,1,1,1,1,1,0,0,1,0,0,1,0)$	5,7,10,12,18	6,8,9,11,13,18	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,1,0,0,0,1,0) \xrightarrow{1r} (0,1,1,0,0,0,0,0,0,0,1,1,0,1,1,0,0)$	5,7,10,12,16,17	6,8,9,11,13,17	2^{-12}
$(0,0,0,0,1,1,1,1,1,1,0,0,1,0,0) \xrightarrow{1r} (0,1,0,1,1,1,1,0,1,0,0,1,0,0,1,0)$	5,7,10,12	6,8,9,11,13,15	$2^{-17.5}$
$(0,0,0,0,1,1,1,1,1,1,0,0,1,1,0) \xrightarrow{1r} (1,0,1,0,0,0,0,0,1,0,1,1,0,1,1,0,0)$	5,7,10,12,16,17,18	6,8,9,11,13,15,17,18	2^{-12}
$(0,0,0,0,1,1,1,1,1,1,0,0,1,1,0) \xrightarrow{1r} (0,1,0,0,0,0,1,0,1,1,1,0,1,1,0,1)$	5,7,10,12,14,17	6,8,9,11,13,17	2^{-12}
$(0,0,0,0,1,1,1,1,1,1,0,0,1,1,0) \xrightarrow{1r} (1,0,1,1,1,1,0,1,0,0,0,1,0,0,1,1)$	5,7,10,12,14,16,18	6,8,9,11,13,18	$2^{-6.5}$
$(0,0,0,0,1,1,1,1,1,1,0,0,1,1,1) \xrightarrow{1r} (1,0,0,0,0,0,1,1,1,1,0,1,1,0,1,1,0,1)$	5,7,10,12,14,17,18	6,8,9,11,13,15,17,18	2^{-12}
$(0,0,0,0,1,1,1,1,1,1,0,0,1,1,1) \xrightarrow{1r} (0,1,1,1,1,1,0,0,0,0,0,1,0,0,1,1)$	5,7,10,12,14,16	6,8,9,11,13,15	$2^{-6.5}$

Table 0.129 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	17,18	4,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	16	4	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	17	4,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	16,18	4,15,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	14	4	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	14,16,17,18	4,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	14,18	4,15,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	14,16,17	4,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	17	4,13,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	16,18	4,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	17,18	4,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	16	4,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	14,18	4,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	14,16,17	4,13,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	14	4,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	14,16,17,18	4,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	12	4	2^{-1}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	12,16,17,18	4,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	12,18	4,15,18	2^{-1}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	12,16,17	4,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	12,14,17,18	4,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	12,14,16	4	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	12,14,17	4,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	12,14,16,18	4,15,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	12,18	4,13,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	12,16,17	4,13,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	12	4,13,15	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	12,16,17,18	4,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	12,14,17	4,13,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	12,14,16,18	4,13,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	12,14,17,18	4,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	12,14,16	4,13,15	$2^{-6.5}$

Table 0.130 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	17	4,11,17	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	16,18	4,11,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	17,18	4,11,15,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	16	4,11,15	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	14,18	4,11,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	14,16,17	4,11,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	14	4,11,15	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	14,16,17,18	4,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	17,18	4,11,13,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	16	4,11,13	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	17	4,11,13,15,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	16,18	4,11,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	14	4,11,13	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	14,16,17,18	4,11,13,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	14,18	4,11,13,15,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	14,16,17	4,11,13,15,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	12,18	4,11,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	12,16,17	4,11,17	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	12	4,11,15	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	12,16,17,18	4,11,15,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	12,14,17	4,11,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	12,14,16,18	4,11,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	12,14,17,18	4,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	12,14,16	4,11,15	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	12	4,11,13	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	12,16,17,18	4,11,13,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	12,18	4,11,13,15,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	12,16,17	4,11,13,15,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	12,14,17,18	4,11,13,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	12,14,16	4,11,13	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	12,14,17	4,11,13,15,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	12,14,16,18	4,11,13,15,18	$2^{-17.5}$

Table 0.131 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	10	4	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	10,16,17,18	4,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	10,18	4,15,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	10,16,17	4,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	10,14,17,18	4,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	10,14,16	4	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	10,14,17	4,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	10,14,16,18	4,15,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	10,18	4,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	10,16,17	4,13,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	10	4,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	10,16,17,18	4,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	10,14,17	4,13,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	10,14,16,18	4,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	10,14,17,18	4,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	10,14,16	4,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	10,12,17,18	4,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	10,12,16	4	2^{-34}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	10,12,17	4,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	10,12,16,18	4,15,18	2^{-34}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	10,12,14	4	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	10,12,14,16,17,18	4,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	10,12,14,18	4,15,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	10,12,14,16,17	4,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	10,12,17	4,13,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	10,12,16,18	4,13,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	10,12,17,18	4,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	10,12,16	4,13,15	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	10,12,14,18	4,13,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	10,12,14,16,17	4,13,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	10,12,14	4,13,15	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	10,12,14,16,17,18	4,13,15,17,18	2^{-23}

Table 0.132 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	10,18	4,11,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	10,16,17	4,11,17	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	10	4,11,15	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	10,16,17,18	4,11,15,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	10,14,17	4,11,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	10,14,16,18	4,11,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	10,14,17,18	4,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	10,14,16	4,11,15	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	10	4,11,13	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	10,16,17,18	4,11,13,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	10,18	4,11,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	10,16,17	4,11,13,15,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	10,14,17,18	4,11,13,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	10,14,16	4,11,13	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	10,14,17	4,11,13,15,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	10,14,16,18	4,11,13,15,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	10,12,17	4,11,17	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	10,12,16,18	4,11,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	10,12,17,18	4,11,15,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	10,12,16	4,11,15	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	10,12,14,18	4,11,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	10,12,14,16,17	4,11,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	10,12,14	4,11,15	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	10,12,14,16,17,18	4,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	10,12,17,18	4,11,13,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	10,12,16	4,11,13	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	10,12,17	4,11,13,15,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	10,12,16,18	4,11,13,15,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	10,12,14	4,11,13	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	10,12,14,16,17,18	4,11,13,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	10,12,14,18	4,11,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	10,12,14,16,17	4,11,13,15,17	2^{-12}

Table 0.133 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	17	4,9,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	16,18	4,9,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	17,18	4,9,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	16	4,9,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	14,18	4,9,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	14,16,17	4,9,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	14	4,9,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	14,16,17,18	4,9,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	17,18	4,9,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	16	4,9,13	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	17	4,9,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	16,18	4,9,13,15,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	14	4,9,13	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	14,16,17,18	4,9,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	14,18	4,9,13,15,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	14,16,17	4,9,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	12,18	4,9,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	12,16,17	4,9,17	2^{-34}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	12	4,9,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	12,16,17,18	4,9,15,17,18	2^{-34}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	12,14,17	4,9,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	12,14,16,18	4,9,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	12,14,17,18	4,9,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	12,14,16	4,9,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	12	4,9,13	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	12,16,17,18	4,9,13,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	12,18	4,9,13,15,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	12,16,17	4,9,13,15,17	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	12,14,17,18	4,9,13,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	12,14,16	4,9,13	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	12,14,17	4,9,13,15,17	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	12,14,16,18	4,9,13,15,18	2^{-23}

Table 0.134 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	17,18	4,9,11,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	16	4,9,11	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	17	4,9,11,15,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	16,18	4,9,11,15,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	14	4,9,11	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	14,16,17,18	4,9,11,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	14,18	4,9,11,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	14,16,17	4,9,11,15,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	17	4,9,11,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	16,18	4,9,11,13,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	17,18	4,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	16	4,9,11,13,15	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	14,18	4,9,11,13,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	14,16,17	4,9,11,13,17	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	14	4,9,11,13,15	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	14,16,17,18	4,9,11,13,15,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	12	4,9,11	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	12,16,17,18	4,9,11,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	12,18	4,9,11,15,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	12,16,17	4,9,11,15,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	12,14,17,18	4,9,11,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	12,14,16	4,9,11	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	12,14,17	4,9,11,15,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	12,14,16,18	4,9,11,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	12,18	4,9,11,13,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	12,16,17	4,9,11,13,17	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	12	4,9,11,13,15	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	12,16,17,18	4,9,11,13,15,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	12,14,17	4,9,11,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	12,14,16,18	4,9,11,13,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	12,14,17,18	4,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	12,14,16	4,9,11,13,15	2^{-12}

Table 0.135 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	10,18	4,9,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	10,16,17	4,9,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	10	4,9,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	10,16,17,18	4,9,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	10,14,17	4,9,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	10,14,16,18	4,9,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	10,14,17,18	4,9,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	10,14,16	4,9,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	10	4,9,13	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	10,16,17,18	4,9,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	10,18	4,9,13,15,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	10,16,17	4,9,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	10,14,17,18	4,9,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	10,14,16	4,9,13	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	10,14,17	4,9,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	10,14,16,18	4,9,13,15,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	10,12,17	4,9,17	2^{-1}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	10,12,16,18	4,9,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	10,12,17,18	4,9,15,17,18	2^{-1}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	10,12,16	4,9,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	10,12,14,18	4,9,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	10,12,14,16,17	4,9,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	10,12,14	4,9,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	10,12,14,16,17,18	4,9,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	10,12,17,18	4,9,13,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	10,12,16	4,9,13	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	10,12,17	4,9,13,15,17	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	10,12,16,18	4,9,13,15,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	10,12,14	4,9,13	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	10,12,14,16,17,18	4,9,13,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	10,12,14,18	4,9,13,15,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	10,12,14,16,17	4,9,13,15,17	$2^{-6.5}$

Table 0.136 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	10	4,9,11	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	10,16,17,18	4,9,11,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	10,18	4,9,11,15,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	10,16,17	4,9,11,15,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	10,14,17,18	4,9,11,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	10,14,16	4,9,11	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	10,14,17	4,9,11,15,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	10,14,16,18	4,9,11,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	10,18	4,9,11,13,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	10,16,17	4,9,11,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	10	4,9,11,13,15	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	10,16,17,18	4,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	10,14,17	4,9,11,13,17	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	10,14,16,18	4,9,11,13,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	10,14,17,18	4,9,11,13,15,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	10,14,16	4,9,11,13,15	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	10,12,17,18	4,9,11,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	10,12,16	4,9,11	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	10,12,17	4,9,11,15,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	10,12,16,18	4,9,11,15,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	10,12,14	4,9,11	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	10,12,14,16,17,18	4,9,11,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	10,12,14,18	4,9,11,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	10,12,14,16,17	4,9,11,15,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	10,12,17	4,9,11,13,17	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	10,12,16,18	4,9,11,13,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	10,12,17,18	4,9,11,13,15,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	10,12,16	4,9,11,13,15	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	10,12,14,18	4,9,11,13,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	10,12,14,16,17	4,9,11,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	10,12,14	4,9,11,13,15	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	10,12,14,16,17,18	4,9,11,13,15,17,18	$2^{-17.5}$

Table 0.137 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	—	4,8	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	16,17,18	4,8,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	18	4,8,15,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	16,17	4,8,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	14,17,18	4,8,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	14,16	4,8	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	14,17	4,8,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	14,16,18	4,8,15,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	18	4,8,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	16,17	4,8,13,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	—	4,8,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	16,17,18	4,8,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	14,17	4,8,13,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	14,16,18	4,8,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	14,17,18	4,8,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	14,16	4,8,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	12,17,18	4,8,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	12,16	4,8	2^{-1}
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	12,17	4,8,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	12,16,18	4,8,15,18	2^{-1}
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	12,14	4,8	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	12,14,16,17,18	4,8,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	12,14,18	4,8,15,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	12,14,16,17	4,8,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	12,17	4,8,13,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	12,16,18	4,8,13,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	12,17,18	4,8,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	12,16	4,8,13,15	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	12,14,18	4,8,13,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	12,14,16,17	4,8,13,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	12,14	4,8,13,15	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	12,14,16,17,18	4,8,13,15,17,18	2^{-12}

Table 0.138 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,1,0,0,0,1,0,0,1,0,0,0,0,0) \xrightarrow{1r} (1,1,1,0,1,1,0,0,1,1,0,1,0,0,1,0)$	18	4,8,11,18	2^{-12}
$(0,0,0,1,0,0,0,1,0,0,1,0,0,0,0,1) \xrightarrow{1r} (0,0,0,1,0,0,1,1,0,0,1,0,1,1,0,0)$	16,17	4,8,11,17	$2^{-6.5}$
$(0,0,0,1,0,0,0,1,0,0,1,0,0,0,1,0) \xrightarrow{1r} (0,0,1,0,1,1,0,1,1,1,0,1,0,0,1,0)$	—	4,8,11,15	2^{-12}
$(0,0,0,1,0,0,0,1,0,0,1,0,0,0,1,1) \xrightarrow{1r} (1,1,0,1,0,0,1,0,0,0,1,0,1,1,0,0)$	16,17,18	4,8,11,15,17,18	$2^{-6.5}$
$(0,0,0,1,0,0,0,1,0,0,1,0,0,1,0,0) \xrightarrow{1r} (0,0,1,1,0,0,0,1,1,0,1,0,1,1,0,1)$	14,17	4,8,11,17	$2^{-17.5}$
$(0,0,0,1,0,0,0,1,0,0,1,0,0,1,0,1) \xrightarrow{1r} (1,1,0,0,1,1,1,0,0,1,0,1,0,0,1,1)$	14,16,18	4,8,11,18	2^{-12}
$(0,0,0,1,0,0,0,1,0,0,1,0,0,1,1,0) \xrightarrow{1r} (1,1,1,1,0,0,0,0,1,0,1,0,1,1,0,1)$	14,17,18	4,8,11,15,17,18	$2^{-17.5}$
$(0,0,0,1,0,0,0,1,0,0,1,0,0,1,1,1) \xrightarrow{1r} (0,0,0,0,1,1,1,1,0,1,0,1,0,0,1,1)$	14,16	4,8,11,15	2^{-12}
$(0,0,0,1,0,0,0,1,0,0,1,0,1,0,0,0) \xrightarrow{1r} (0,0,1,1,1,0,0,0,1,0,0,1,0,0,1,0)$	—	4,8,11,13	$2^{-17.5}$
$(0,0,0,1,0,0,0,1,0,0,1,0,1,0,0,1) \xrightarrow{1r} (1,1,0,0,0,1,1,1,0,1,1,0,1,1,0,0)$	16,17,18	4,8,11,13,17,18	2^{-12}
$(0,0,0,1,0,0,0,1,0,0,1,0,1,0,1,0) \xrightarrow{1r} (1,1,1,1,1,0,0,1,1,0,0,1,0,0,1,0)$	18	4,8,11,13,15,18	$2^{-17.5}$
$(0,0,0,1,0,0,0,1,0,0,1,0,1,0,1,1) \xrightarrow{1r} (0,0,0,0,0,1,1,0,0,1,1,0,1,1,0,0)$	16,17	4,8,11,13,15,17	2^{-12}
$(0,0,0,1,0,0,0,1,0,0,1,0,1,1,0,0) \xrightarrow{1r} (1,1,1,0,0,1,0,1,1,1,1,0,1,1,0,1)$	14,17,18	4,8,11,13,17,18	2^{-12}
$(0,0,0,1,0,0,0,1,0,0,1,0,1,1,0,1) \xrightarrow{1r} (0,0,0,1,1,0,1,0,0,0,0,1,0,0,1,1)$	14,16	4,8,11,13	$2^{-6.5}$
$(0,0,0,1,0,0,0,1,0,0,1,0,1,1,1,0) \xrightarrow{1r} (0,0,1,0,0,1,0,0,1,1,1,0,1,1,0,1)$	14,17	4,8,11,13,15,17	2^{-12}
$(0,0,0,1,0,0,0,1,0,0,1,0,1,1,1,1) \xrightarrow{1r} (1,1,0,1,1,0,1,1,0,0,0,1,0,0,1,1)$	14,16,18	4,8,11,13,15,18	$2^{-6.5}$
$(0,0,0,1,0,0,0,1,0,0,1,1,0,0,0,0) \xrightarrow{1r} (0,0,1,1,0,0,1,1,1,0,0,0,1,1,0,1)$	12,17	4,8,11,17	$2^{-28.5}$
$(0,0,0,1,0,0,0,1,0,0,1,1,0,0,0,1) \xrightarrow{1r} (1,1,0,0,1,1,0,0,0,1,1,1,0,0,1,1)$	12,16,18	4,8,11,18	2^{-12}
$(0,0,0,1,0,0,0,1,0,0,1,1,0,0,1,0) \xrightarrow{1r} (1,1,1,1,0,0,1,0,1,0,0,0,1,1,0,1)$	12,17,18	4,8,11,15,17,18	$2^{-28.5}$
$(0,0,0,1,0,0,0,1,0,0,1,1,0,0,1,1) \xrightarrow{1r} (0,0,0,0,1,1,0,1,0,1,1,1,0,0,1,1)$	12,16	4,8,11,15	2^{-12}
$(0,0,0,1,0,0,0,1,0,0,1,1,0,1,0,0) \xrightarrow{1r} (1,1,1,0,1,1,1,0,1,1,1,1,0,0,1,0)$	12,14,18	4,8,11,18	2^{-12}
$(0,0,0,1,0,0,0,1,0,0,1,1,0,1,0,1) \xrightarrow{1r} (0,0,0,1,0,0,0,1,0,0,0,0,1,1,0,0)$	12,14,16,17	4,8,11,17	$2^{-17.5}$
$(0,0,0,1,0,0,0,1,0,0,1,1,0,1,1,0) \xrightarrow{1r} (0,0,1,0,1,1,1,1,1,1,1,1,1,0,0,1,0)$	12,14	4,8,11,15	2^{-12}
$(0,0,0,1,0,0,0,1,0,0,1,1,0,1,1,1) \xrightarrow{1r} (1,1,0,1,0,0,0,0,0,0,0,0,0,1,1,0,0)$	12,14,16,17,18	4,8,11,15,17,18	$2^{-17.5}$
$(0,0,0,1,0,0,0,1,0,0,1,1,1,0,0,0) \xrightarrow{1r} (1,1,1,0,0,1,1,1,1,1,1,0,0,1,1,0,1)$	12,17,18	4,8,11,13,17,18	2^{-23}
$(0,0,0,1,0,0,0,1,0,0,1,1,1,0,0,1) \xrightarrow{1r} (0,0,0,1,1,0,0,0,0,0,0,1,1,0,0,1,1)$	12,16	4,8,11,13	$2^{-6.5}$
$(0,0,0,1,0,0,0,1,0,0,1,1,1,0,1,0) \xrightarrow{1r} (0,0,1,0,0,1,1,0,1,1,0,0,1,1,0,1)$	12,17	4,8,11,13,15,17	2^{-23}
$(0,0,0,1,0,0,0,1,0,0,1,1,1,0,1,1) \xrightarrow{1r} (1,1,0,1,1,0,0,1,0,0,1,1,0,0,1,1)$	12,16,18	4,8,11,13,15,18	$2^{-6.5}$
$(0,0,0,1,0,0,0,1,0,0,1,1,1,1,0,0) \xrightarrow{1r} (0,0,1,1,1,0,1,0,1,0,1,0,1,1,0,0,1,0)$	12,14	4,8,11,13	$2^{-17.5}$
$(0,0,0,1,0,0,0,1,0,0,1,1,1,1,0,1) \xrightarrow{1r} (1,1,0,0,0,1,0,1,0,1,0,1,0,0,1,1,0,0)$	12,14,16,17,18	4,8,11,13,17,18	2^{-23}
$(0,0,0,1,0,0,0,1,0,0,1,1,1,1,1,0) \xrightarrow{1r} (1,1,1,1,1,0,1,1,1,0,1,1,0,0,1,0,0)$	12,14,18	4,8,11,13,15,18	$2^{-17.5}$
$(0,0,0,1,0,0,0,1,0,0,1,1,1,1,1,1) \xrightarrow{1r} (0,0,0,0,0,1,0,0,0,1,0,0,1,1,0,0)$	12,14,16,17	4,8,11,13,15,17	2^{-23}

Table 0.139 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,1,0,0,0,1,0,1,0,0,0,0,0,0) \xrightarrow{1r} (1,1,0,1,1,1,0,1,1,1,0,1,0,1,0,1)$	10,17,18	4,8,17,18	$2^{-17.5}$
$(0,0,0,1,0,0,0,1,0,1,0,0,0,0,0,1) \xrightarrow{1r} (0,0,1,0,0,0,1,0,0,0,1,0,1,0,1,1)$	10,16	4,8	2^{-12}
$(0,0,0,1,0,0,0,1,0,1,0,0,0,0,1,0) \xrightarrow{1r} (0,0,0,1,1,1,0,0,1,1,0,1,0,1,0,1)$	10,17	4,8,15,17	$2^{-17.5}$
$(0,0,0,1,0,0,0,1,0,1,0,0,0,0,1,1) \xrightarrow{1r} (1,1,1,0,0,0,1,1,0,0,1,0,1,0,1,1)$	10,16,18	4,8,15,18	2^{-12}
$(0,0,0,1,0,0,0,1,0,1,0,0,0,1,0,0) \xrightarrow{1r} (0,0,0,0,0,0,0,0,1,0,1,0,1,0,1,0)$	10,14	4,8	2^{-23}
$(0,0,0,1,0,0,0,1,0,1,0,0,0,1,0,1) \xrightarrow{1r} (1,1,1,1,1,1,1,1,0,1,0,1,0,1,0,0)$	10,14,16,17,18	4,8,17,18	$2^{-17.5}$
$(0,0,0,1,0,0,0,1,0,1,0,0,0,1,1,0) \xrightarrow{1r} (1,1,0,0,0,0,0,1,1,0,1,0,1,0,1,0)$	10,14,18	4,8,15,18	2^{-23}
$(0,0,0,1,0,0,0,1,0,1,0,0,0,1,1,1) \xrightarrow{1r} (0,0,1,1,1,1,1,0,0,1,0,1,0,1,0,0)$	10,14,16,17	4,8,15,17	$2^{-17.5}$
$(0,0,0,1,0,0,0,1,0,1,0,0,1,0,0,0) \xrightarrow{1r} (0,0,0,0,1,0,0,1,1,0,0,1,0,1,0,1)$	10,17	4,8,13,17	2^{-23}
$(0,0,0,1,0,0,0,1,0,1,0,0,1,0,0,1) \xrightarrow{1r} (1,1,1,1,0,1,1,0,0,1,1,0,1,0,1,1)$	10,16,18	4,8,13,18	$2^{-17.5}$
$(0,0,0,1,0,0,0,1,0,1,0,0,1,0,1,0) \xrightarrow{1r} (1,1,0,0,1,0,0,0,1,0,0,1,0,1,0,1)$	10,17,18	4,8,13,15,17,18	2^{-23}
$(0,0,0,1,0,0,0,1,0,1,0,0,1,0,1,1) \xrightarrow{1r} (0,0,1,1,0,1,1,1,0,1,1,0,1,0,1,1)$	10,16	4,8,13,15	$2^{-17.5}$
$(0,0,0,1,0,0,0,1,0,1,0,0,1,1,0,0) \xrightarrow{1r} (1,1,0,1,0,1,0,0,1,1,1,0,1,0,1,0)$	10,14,18	4,8,13,18	$2^{-17.5}$
$(0,0,0,1,0,0,0,1,0,1,0,0,1,1,0,1) \xrightarrow{1r} (0,0,1,0,1,0,1,1,0,0,0,1,0,1,0,0)$	10,14,16,17	4,8,13,17	2^{-12}
$(0,0,0,1,0,0,0,1,0,1,0,0,1,1,1,0) \xrightarrow{1r} (0,0,0,1,0,1,0,1,1,1,1,0,1,0,1,0)$	10,14	4,8,13,15	$2^{-17.5}$
$(0,0,0,1,0,0,0,1,0,1,0,0,1,1,1,1) \xrightarrow{1r} (1,1,1,0,1,0,1,0,0,0,0,1,0,1,0,0)$	10,14,16,17,18	4,8,13,15,17,18	2^{-12}
$(0,0,0,1,0,0,0,1,0,1,0,1,0,0,0,0) \xrightarrow{1r} (0,0,0,0,0,0,1,0,1,0,0,0,1,0,1,0)$	10,12	4,8	2^{-34}
$(0,0,0,1,0,0,0,1,0,1,0,1,0,0,0,1) \xrightarrow{1r} (1,1,1,1,1,1,0,1,0,1,1,1,0,1,0,0)$	10,12,16,17,18	4,8,17,18	$2^{-17.5}$
$(0,0,0,1,0,0,0,1,0,1,0,1,0,0,1,0) \xrightarrow{1r} (1,1,0,0,0,0,1,1,1,0,0,0,1,0,1,0)$	10,12,18	4,8,15,18	2^{-34}
$(0,0,0,1,0,0,0,1,0,1,0,1,0,0,1,1) \xrightarrow{1r} (0,0,1,1,1,1,0,0,0,1,1,1,0,1,0,0)$	10,12,16,17	4,8,15,17	$2^{-17.5}$
$(0,0,0,1,0,0,0,1,0,1,0,1,0,1,0,0) \xrightarrow{1r} (1,1,0,1,1,1,1,1,1,1,1,1,0,1,0,1)$	10,12,14,17,18	4,8,17,18	$2^{-17.5}$
$(0,0,0,1,0,0,0,1,0,1,0,1,0,1,0,1) \xrightarrow{1r} (0,0,1,0,0,0,0,0,0,0,0,0,1,0,1,1)$	10,12,14,16	4,8	2^{-23}
$(0,0,0,1,0,0,0,1,0,1,0,1,0,1,1,0) \xrightarrow{1r} (0,0,0,1,1,1,1,0,1,1,1,1,0,1,0,1)$	10,12,14,17	4,8,15,17	$2^{-17.5}$
$(0,0,0,1,0,0,0,1,0,1,0,1,0,1,1,1) \xrightarrow{1r} (1,1,1,0,0,0,0,1,0,0,0,0,1,0,1,1)$	10,12,14,16,18	4,8,15,18	2^{-23}
$(0,0,0,1,0,0,0,1,0,1,0,1,1,0,0,0) \xrightarrow{1r} (1,1,0,1,0,1,1,0,1,1,0,1,1,0,1,0)$	10,12,18	4,8,13,18	$2^{-28.5}$
$(0,0,0,1,0,0,0,1,0,1,0,1,1,0,0,1) \xrightarrow{1r} (0,0,1,0,1,0,0,1,0,0,1,0,0,1,1,0,0,0)$	10,12,16,17	4,8,13,17	2^{-12}
$(0,0,0,1,0,0,0,1,0,1,0,1,1,0,1,0) \xrightarrow{1r} (0,0,0,1,0,1,1,1,1,1,0,0,1,0,1,0)$	10,12	4,8,13,15	$2^{-28.5}$
$(0,0,0,1,0,0,0,1,0,1,0,1,1,0,1,1) \xrightarrow{1r} (1,1,1,0,1,0,0,0,0,0,1,1,0,1,0,0)$	10,12,16,17,18	4,8,13,15,17,18	2^{-12}
$(0,0,0,1,0,0,0,1,0,1,0,1,1,1,0,0) \xrightarrow{1r} (0,0,0,0,1,0,1,1,1,0,1,1,0,1,0,1)$	10,12,14,17	4,8,13,17	2^{-23}
$(0,0,0,1,0,0,0,1,0,1,0,1,1,1,0,1) \xrightarrow{1r} (1,1,1,1,0,1,0,0,0,1,0,0,1,0,1,1)$	10,12,14,16,18	4,8,13,18	$2^{-28.5}$
$(0,0,0,1,0,0,0,1,0,1,0,1,1,1,1,0) \xrightarrow{1r} (1,1,0,0,1,0,1,0,1,0,1,0,1,1,0,1)$	10,12,14,17,18	4,8,13,15,17,18	2^{-23}
$(0,0,0,1,0,0,0,1,0,1,0,1,1,1,1,1) \xrightarrow{1r} (0,0,1,1,0,1,0,1,0,1,0,1,0,1,0,1)$	10,12,14,16	4,8,13,15	$2^{-28.5}$

Table 0.140 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	10,17	4,8,11,17	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	10,16,18	4,8,11,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	10,17,18	4,8,11,15,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	10,16	4,8,11,15	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	10,14,18	4,8,11,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	10,14,16,17	4,8,11,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	10,14	4,8,11,15	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	10,14,16,17,18	4,8,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	10,17,18	4,8,11,13,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	10,16	4,8,11,13	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	10,17	4,8,11,13,15,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	10,16,18	4,8,11,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	10,14	4,8,11,13	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	10,14,16,17,18	4,8,11,13,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	10,14,18	4,8,11,13,15,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	10,14,16,17	4,8,11,13,15,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	10,12,18	4,8,11,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	10,12,16,17	4,8,11,17	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	10,12	4,8,11,15	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	10,12,16,17,18	4,8,11,15,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	10,12,14,17	4,8,11,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	10,12,14,16,18	4,8,11,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	10,12,14,17,18	4,8,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	10,12,14,16	4,8,11,15	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	10,12	4,8,11,13	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	10,12,16,17,18	4,8,11,13,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	10,12,18	4,8,11,13,15,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	10,12,16,17	4,8,11,13,15,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	10,12,14,17,18	4,8,11,13,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	10,12,14,16	4,8,11,13	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	10,12,14,17	4,8,11,13,15,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	10,12,14,16,18	4,8,11,13,15,18	$2^{-17.5}$

Table 0.141 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	18	4,8,9,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	16,17	4,8,9,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	—	4,8,9,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	16,17,18	4,8,9,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	14,17	4,8,9,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	14,16,18	4,8,9,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	14,17,18	4,8,9,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	14,16	4,8,9,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	—	4,8,9,13	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	16,17,18	4,8,9,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	18	4,8,9,13,15,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	16,17	4,8,9,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	14,17,18	4,8,9,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	14,16	4,8,9,13	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	14,17	4,8,9,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	14,16,18	4,8,9,13,15,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	12,17	4,8,9,17	2^{-34}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	12,16,18	4,8,9,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	12,17,18	4,8,9,15,17,18	2^{-34}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	12,16	4,8,9,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	12,14,18	4,8,9,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	12,14,16,17	4,8,9,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	12,14	4,8,9,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	12,14,16,17,18	4,8,9,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	12,17,18	4,8,9,13,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	12,16	4,8,9,13	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	12,17	4,8,9,13,15,17	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	12,16,18	4,8,9,13,15,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	12,14	4,8,9,13	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	12,14,16,17,18	4,8,9,13,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	12,14,18	4,8,9,13,15,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	12,14,16,17	4,8,9,13,15,17	$2^{-28.5}$

Table 0.142 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	—	4,8,9,11	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	16,17,18	4,8,9,11,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	18	4,8,9,11,15,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	16,17	4,8,9,11,15,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	14,17,18	4,8,9,11,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	14,16	4,8,9,11	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	14,17	4,8,9,11,15,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	14,16,18	4,8,9,11,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	18	4,8,9,11,13,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	16,17	4,8,9,11,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	—	4,8,9,11,13,15	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	16,17,18	4,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	14,17	4,8,9,11,13,17	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	14,16,18	4,8,9,11,13,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	14,17,18	4,8,9,11,13,15,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	14,16	4,8,9,11,13,15	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	12,17,18	4,8,9,11,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	12,16	4,8,9,11	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	12,17	4,8,9,11,15,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	12,16,18	4,8,9,11,15,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	12,14	4,8,9,11	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	12,14,16,17,18	4,8,9,11,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	12,14,18	4,8,9,11,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	12,14,16,17	4,8,9,11,15,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	12,17	4,8,9,11,13,17	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	12,16,18	4,8,9,11,13,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	12,17,18	4,8,9,11,13,15,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	12,16	4,8,9,11,13,15	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	12,14,18	4,8,9,11,13,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	12,14,16,17	4,8,9,11,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	12,14	4,8,9,11,13,15	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	12,14,16,17,18	4,8,9,11,13,15,17,18	$2^{-17.5}$

Table 0.143 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	10,17	4,8,9,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	10,16,18	4,8,9,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	10,17,18	4,8,9,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	10,16	4,8,9,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	10,14,18	4,8,9,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	10,14,16,17	4,8,9,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	10,14	4,8,9,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	10,14,16,17,18	4,8,9,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	10,17,18	4,8,9,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	10,16	4,8,9,13	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	10,17	4,8,9,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	10,16,18	4,8,9,13,15,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	10,14	4,8,9,13	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	10,14,16,17,18	4,8,9,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	10,14,18	4,8,9,13,15,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	10,14,16,17	4,8,9,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	10,12,18	4,8,9,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	10,12,16,17	4,8,9,17	2^{-1}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	10,12	4,8,9,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	10,12,16,17,18	4,8,9,15,17,18	2^{-1}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	10,12,14,17	4,8,9,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	10,12,14,16,18	4,8,9,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	10,12,14,17,18	4,8,9,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	10,12,14,16	4,8,9,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	10,12	4,8,9,13	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	10,12,16,17,18	4,8,9,13,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	10,12,18	4,8,9,13,15,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	10,12,16,17	4,8,9,13,15,17	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	10,12,14,17,18	4,8,9,13,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	10,12,14,16	4,8,9,13	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	10,12,14,17	4,8,9,13,15,17	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	10,12,14,16,18	4,8,9,13,15,18	2^{-12}

Table 0.144 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	10,17,18	4,8,9,11,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	10,16	4,8,9,11	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	10,17	4,8,9,11,15,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	10,16,18	4,8,9,11,15,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	10,14	4,8,9,11	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	10,14,16,17,18	4,8,9,11,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	10,14,18	4,8,9,11,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	10,14,16,17	4,8,9,11,15,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	10,17	4,8,9,11,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	10,16,18	4,8,9,11,13,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	10,17,18	4,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	10,16	4,8,9,11,13,15	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	10,14,18	4,8,9,11,13,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	10,14,16,17	4,8,9,11,13,17	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	10,14	4,8,9,11,13,15	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	10,14,16,17,18	4,8,9,11,13,15,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	10,12	4,8,9,11	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	10,12,16,17,18	4,8,9,11,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	10,12,18	4,8,9,11,15,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	10,12,16,17	4,8,9,11,15,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	10,12,14,17,18	4,8,9,11,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	10,12,14,16	4,8,9,11	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	10,12,14,17	4,8,9,11,15,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	10,12,14,16,18	4,8,9,11,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	10,12,18	4,8,9,11,13,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	10,12,16,17	4,8,9,11,13,17	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	10,12	4,8,9,11,13,15	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	10,12,16,17,18	4,8,9,11,13,15,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	10,12,14,17	4,8,9,11,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	10,12,14,16,18	4,8,9,11,13,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	10,12,14,17,18	4,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	10,12,14,16	4,8,9,11,13,15	2^{-23}

Table 0.145 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	7,17	4,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	7,16,18	4,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	7,17,18	4,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	7,16	4,15	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	7,14,18	4,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	7,14,16,17	4,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	7,14	4,15	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	7,14,16,17,18	4,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	7,17,18	4,13,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	7,16	4,13	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	7,17	4,13,15,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	7,16,18	4,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	7,14	4,13	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	7,14,16,17,18	4,13,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	7,14,18	4,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	7,14,16,17	4,13,15,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	7,12,18	4,18	2^{-1}
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	7,12,16,17	4,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	7,12	4,15	2^{-1}
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	7,12,16,17,18	4,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	7,12,14,17	4,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	7,12,14,16,18	4,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	7,12,14,17,18	4,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	7,12,14,16	4,15	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	7,12	4,13	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	7,12,16,17,18	4,13,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	7,12,18	4,13,15,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	7,12,16,17	4,13,15,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	7,12,14,17,18	4,13,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	7,12,14,16	4,13	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	7,12,14,17	4,13,15,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	7,12,14,16,18	4,13,15,18	$2^{-6.5}$

Table 0.146 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,1,0,0,1,0,0,0,1,0,0,0,0,0) \xrightarrow{1r} (1,1,0,1,0,0,1,1,0,0,1,0,1,0,1,1)$	7,17,18	4,11,17,18	$2^{-6.5}$
$(0,0,0,1,0,0,1,0,0,0,1,0,0,0,0,1) \xrightarrow{1r} (0,0,1,0,1,1,0,0,1,1,0,1,0,1,0,1)$	7,16	4,11	2^{-12}
$(0,0,0,1,0,0,1,0,0,0,1,0,0,0,1,0) \xrightarrow{1r} (0,0,0,1,0,0,1,0,0,0,1,0,1,0,1,1)$	7,17	4,11,15,17	$2^{-6.5}$
$(0,0,0,1,0,0,1,0,0,0,1,0,0,0,1,1) \xrightarrow{1r} (1,1,1,0,1,1,0,1,1,1,0,1,0,1,0,1)$	7,16,18	4,11,15,18	2^{-12}
$(0,0,0,1,0,0,1,0,0,0,1,0,0,1,0,0) \xrightarrow{1r} (0,0,0,0,1,1,1,0,0,1,0,1,0,1,0,0)$	7,14	4,11	2^{-12}
$(0,0,0,1,0,0,1,0,0,0,1,0,0,1,0,1) \xrightarrow{1r} (1,1,1,1,0,0,0,1,1,0,1,0,1,0,1,0)$	7,14,16,17,18	4,11,17,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,0,0,0,1,0,0,1,1,0) \xrightarrow{1r} (1,1,0,0,1,1,1,1,0,1,0,1,0,1,0,0)$	7,14,18	4,11,15,18	2^{-12}
$(0,0,0,1,0,0,1,0,0,0,1,0,0,1,1,1) \xrightarrow{1r} (0,0,1,1,0,0,0,0,1,0,1,0,1,0,1,0)$	7,14,16,17	4,11,15,17	$2^{-17.5}$
$(0,0,0,1,0,0,1,0,0,0,1,0,1,0,0,0) \xrightarrow{1r} (0,0,0,0,0,1,1,1,0,1,1,0,1,0,1,1)$	7,17	4,11,13,17	2^{-12}
$(0,0,0,1,0,0,1,0,0,0,1,0,1,0,0,1) \xrightarrow{1r} (1,1,1,1,1,0,0,0,1,0,0,1,0,1,0,1)$	7,16,18	4,11,13,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,0,0,0,1,0,1,0,1,0) \xrightarrow{1r} (1,1,0,0,0,1,1,0,0,1,1,0,1,0,1,1)$	7,17,18	4,11,13,15,17,18	2^{-12}
$(0,0,0,1,0,0,1,0,0,0,1,0,1,0,1,1) \xrightarrow{1r} (0,0,1,1,1,0,0,1,1,0,0,1,0,1,0,1)$	7,16	4,11,13,15	$2^{-17.5}$
$(0,0,0,1,0,0,1,0,0,0,1,0,1,1,0,0) \xrightarrow{1r} (1,1,0,1,1,0,1,0,0,0,0,1,0,1,0,0)$	7,14,18	4,11,13,18	$2^{-6.5}$
$(0,0,0,1,0,0,1,0,0,0,1,0,1,1,0,1) \xrightarrow{1r} (0,0,1,0,0,1,0,1,1,1,1,0,1,0,1,0)$	7,14,16,17	4,11,13,17	2^{-12}
$(0,0,0,1,0,0,1,0,0,0,1,0,1,1,1,0) \xrightarrow{1r} (0,0,0,1,1,0,1,1,0,0,0,1,0,1,0,0)$	7,14	4,11,13,15	$2^{-6.5}$
$(0,0,0,1,0,0,1,0,0,0,1,0,1,1,1,1) \xrightarrow{1r} (1,1,1,0,0,1,0,0,1,1,1,0,1,0,1,0)$	7,14,16,17,18	4,11,13,15,17,18	2^{-12}
$(0,0,0,1,0,0,1,0,0,0,1,1,0,0,0,0) \xrightarrow{1r} (0,0,0,0,1,1,0,0,0,1,1,1,0,1,0,0)$	7,12	4,11	2^{-12}
$(0,0,0,1,0,0,1,0,0,0,1,1,0,0,0,1) \xrightarrow{1r} (1,1,1,1,0,0,1,1,1,0,0,0,1,0,1,0)$	7,12,16,17,18	4,11,17,18	$2^{-28.5}$
$(0,0,0,1,0,0,1,0,0,0,1,1,0,0,1,0) \xrightarrow{1r} (1,1,0,0,1,1,0,1,0,1,1,1,0,1,0,0)$	7,12,18	4,11,15,18	2^{-12}
$(0,0,0,1,0,0,1,0,0,0,1,1,0,0,1,1) \xrightarrow{1r} (0,0,1,1,0,0,1,0,1,0,0,0,1,0,1,0)$	7,12,16,17	4,11,15,17	$2^{-28.5}$
$(0,0,0,1,0,0,1,0,0,0,1,1,0,1,0,0) \xrightarrow{1r} (1,1,0,1,0,0,0,1,0,0,0,0,1,0,1,1)$	7,12,14,17,18	4,11,17,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,0,0,0,1,1,0,1,0,1) \xrightarrow{1r} (0,0,1,0,1,1,1,0,1,1,1,1,0,1,0,1)$	7,12,14,16	4,11	2^{-12}
$(0,0,0,1,0,0,1,0,0,0,1,1,0,1,1,0) \xrightarrow{1r} (0,0,0,1,0,0,0,0,0,0,0,0,1,0,1,1)$	7,12,14,17	4,11,15,17	$2^{-17.5}$
$(0,0,0,1,0,0,1,0,0,0,1,1,0,1,1,1) \xrightarrow{1r} (1,1,1,0,1,1,1,1,1,1,1,1,1,0,1,0)$	7,12,14,16,18	4,11,15,18	2^{-12}
$(0,0,0,1,0,0,1,0,0,0,1,1,1,0,0,0) \xrightarrow{1r} (1,1,0,1,1,0,0,0,0,0,1,1,0,1,0,0)$	7,12,18	4,11,13,18	$2^{-6.5}$
$(0,0,0,1,0,0,1,0,0,0,1,1,1,0,0,1) \xrightarrow{1r} (0,0,1,0,0,1,1,1,1,1,0,0,1,0,1,0)$	7,12,16,17	4,11,13,17	2^{-23}
$(0,0,0,1,0,0,1,0,0,0,1,1,1,0,1,0) \xrightarrow{1r} (0,0,0,1,1,0,0,1,0,0,1,1,0,1,0,0)$	7,12	4,11,13,15	$2^{-6.5}$
$(0,0,0,1,0,0,1,0,0,0,1,1,1,0,1,1) \xrightarrow{1r} (1,1,1,0,0,1,1,0,1,1,0,0,1,0,1,0)$	7,12,16,17,18	4,11,13,15,17,18	2^{-23}
$(0,0,0,1,0,0,1,0,0,0,1,1,1,1,0,0) \xrightarrow{1r} (0,0,0,0,0,1,0,1,0,1,0,1,0,1,0,1)$	7,12,14,17	4,11,13,17	2^{-23}
$(0,0,0,1,0,0,1,0,0,0,1,1,1,1,0,1) \xrightarrow{1r} (1,1,1,1,1,0,1,0,1,0,1,1,0,1,0,1)$	7,12,14,16,18	4,11,13,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,0,0,0,1,1,1,1,1,0) \xrightarrow{1r} (1,1,0,0,0,1,0,0,0,1,0,0,1,0,1,1)$	7,12,14,17,18	4,11,13,15,17,18	2^{-23}
$(0,0,0,1,0,0,1,0,0,0,1,1,1,1,1,1) \xrightarrow{1r} (0,0,1,1,1,0,1,1,1,0,1,1,0,1,0,1)$	7,12,14,16	4,11,13,15	$2^{-17.5}$

Table 0.147 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,1,0,0,1,0,0,1,0,0,0,0,0,0) \xrightarrow{1r} (1,1,1,0,0,0,1,0,0,0,1,0,1,1,0,0)$	7,10,18	4,18	2^{-12}
$(0,0,0,1,0,0,1,0,0,1,0,0,0,0,0,1) \xrightarrow{1r} (0,0,0,1,1,1,0,1,1,1,0,1,0,0,1,0)$	7,10,16,17	4,17	$2^{-17.5}$
$(0,0,0,1,0,0,1,0,0,1,0,0,0,0,1,0) \xrightarrow{1r} (0,0,1,0,0,0,1,1,0,0,1,0,1,1,0,0)$	7,10	4,15	2^{-12}
$(0,0,0,1,0,0,1,0,0,1,0,0,0,0,1,1) \xrightarrow{1r} (1,1,0,1,1,1,0,0,1,1,0,1,0,0,1,0)$	7,10,16,17,18	4,15,17,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,0,0,1,0,0,0,1,0,0) \xrightarrow{1r} (0,0,1,1,1,1,1,0,1,0,1,0,1,0,0,1,1)$	7,10,14,17	4,17	$2^{-17.5}$
$(0,0,0,1,0,0,1,0,0,1,0,0,0,1,0,1) \xrightarrow{1r} (1,1,0,0,0,0,0,0,1,0,1,0,1,1,0,1)$	7,10,14,16,18	4,18	2^{-23}
$(0,0,0,1,0,0,1,0,0,1,0,0,0,1,1,0) \xrightarrow{1r} (1,1,1,1,1,1,1,0,0,1,0,1,0,0,1,1)$	7,10,14,17,18	4,15,17,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,0,0,1,0,0,0,1,1,1) \xrightarrow{1r} (0,0,0,0,0,0,0,0,1,1,0,1,0,1,1,0,1)$	7,10,14,16	4,15	2^{-23}
$(0,0,0,1,0,0,1,0,0,1,0,0,1,0,0,0) \xrightarrow{1r} (0,0,1,1,0,1,1,0,0,1,1,0,1,1,0,0)$	7,10	4,13	$2^{-17.5}$
$(0,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1) \xrightarrow{1r} (1,1,0,0,1,0,0,1,1,0,0,1,0,0,1,0)$	7,10,16,17,18	4,13,17,18	2^{-23}
$(0,0,0,1,0,0,1,0,0,1,0,0,1,0,1,0) \xrightarrow{1r} (1,1,1,1,0,1,1,1,0,1,1,0,1,1,0,0)$	7,10,18	4,13,15,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,0,0,1,0,0,1,0,1,1) \xrightarrow{1r} (0,0,0,0,1,0,0,0,1,0,0,1,0,0,1,0)$	7,10,16,17	4,13,15,17	2^{-23}
$(0,0,0,1,0,0,1,0,0,1,0,0,1,1,0,0) \xrightarrow{1r} (1,1,1,0,1,0,1,1,0,0,0,1,0,0,1,1)$	7,10,14,17,18	4,13,17,18	2^{-12}
$(0,0,0,1,0,0,1,0,0,1,0,0,1,1,0,1) \xrightarrow{1r} (0,0,0,1,0,1,0,0,1,1,1,0,1,1,0,1)$	7,10,14,16	4,13	$2^{-17.5}$
$(0,0,0,1,0,0,1,0,0,1,0,0,1,1,1,0) \xrightarrow{1r} (0,0,1,0,1,0,1,0,0,0,0,1,0,0,1,1)$	7,10,14,17	4,13,15,17	2^{-12}
$(0,0,0,1,0,0,1,0,0,1,0,0,1,1,1,1) \xrightarrow{1r} (1,1,0,1,0,1,0,1,1,1,1,0,1,1,0,1)$	7,10,14,16,18	4,13,15,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,0,0,1,0,1,0,0,0,0) \xrightarrow{1r} (0,0,1,1,1,1,0,1,0,1,1,1,0,0,1,1)$	7,10,12,17	4,17	$2^{-17.5}$
$(0,0,0,1,0,0,1,0,0,1,0,1,0,0,0,1) \xrightarrow{1r} (1,1,0,0,0,0,1,0,1,0,0,0,1,1,0,1)$	7,10,12,16,18	4,18	2^{-34}
$(0,0,0,1,0,0,1,0,0,1,0,1,0,0,1,0) \xrightarrow{1r} (1,1,1,1,1,1,0,0,0,1,1,1,0,0,1,1)$	7,10,12,17,18	4,15,17,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,0,0,1,0,1,0,0,1,1) \xrightarrow{1r} (0,0,0,0,0,0,1,1,1,0,0,0,1,1,0,1)$	7,10,12,16	4,15	2^{-34}
$(0,0,0,1,0,0,1,0,0,1,0,1,0,1,0,0) \xrightarrow{1r} (1,1,1,0,0,0,0,0,0,0,0,0,0,1,1,0,0)$	7,10,12,14,18	4,18	2^{-23}
$(0,0,0,1,0,0,1,0,0,1,0,1,0,1,0,1) \xrightarrow{1r} (0,0,0,1,1,1,1,1,1,1,1,1,1,0,0,1,0)$	7,10,12,14,16,17	4,17	$2^{-17.5}$
$(0,0,0,1,0,0,1,0,0,1,0,1,0,1,1,0) \xrightarrow{1r} (0,0,1,0,0,0,0,1,0,0,0,0,1,1,0,0)$	7,10,12,14	4,15	2^{-23}
$(0,0,0,1,0,0,1,0,0,1,0,1,0,1,1,1) \xrightarrow{1r} (1,1,0,1,1,1,1,0,1,1,1,1,1,0,0,1,0)$	7,10,12,14,16,17,18	4,15,17,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,0,0,1,0,1,1,0,0,0) \xrightarrow{1r} (1,1,1,0,1,0,0,1,0,0,1,1,0,0,1,1)$	7,10,12,17,18	4,13,17,18	2^{-12}
$(0,0,0,1,0,0,1,0,0,1,0,1,1,0,0,1) \xrightarrow{1r} (0,0,0,1,0,1,1,0,1,1,1,0,0,1,1,0,1)$	7,10,12,16	4,13	$2^{-28.5}$
$(0,0,0,1,0,0,1,0,0,1,0,1,1,0,1,0) \xrightarrow{1r} (0,0,1,0,1,0,0,0,0,0,0,1,1,0,0,1,1)$	7,10,12,17	4,13,15,17	2^{-12}
$(0,0,0,1,0,0,1,0,0,1,0,1,1,0,1,1) \xrightarrow{1r} (1,1,0,1,0,1,1,1,1,1,0,0,1,1,0,1)$	7,10,12,16,18	4,13,15,18	$2^{-28.5}$
$(0,0,0,1,0,0,1,0,0,1,0,1,1,1,0,0) \xrightarrow{1r} (0,0,1,1,0,1,0,0,0,1,0,0,1,1,0,0)$	7,10,12,14	4,13	$2^{-28.5}$
$(0,0,0,1,0,0,1,0,0,1,0,1,1,1,0,1) \xrightarrow{1r} (1,1,0,0,1,0,1,1,1,0,1,1,0,0,1,0)$	7,10,12,14,16,17,18	4,13,17,18	2^{-23}
$(0,0,0,1,0,0,1,0,0,1,0,1,1,1,1,0) \xrightarrow{1r} (1,1,1,1,0,1,0,1,0,1,0,0,1,1,0,0)$	7,10,12,14,18	4,13,15,18	$2^{-28.5}$
$(0,0,0,1,0,0,1,0,0,1,0,1,1,1,1,1) \xrightarrow{1r} (0,0,0,0,1,0,1,0,1,0,1,1,0,0,1,0)$	7,10,12,14,16,17	4,13,15,17	2^{-23}

Table 0.148 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	7,10	4,11	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	7,10,16,17,18	4,11,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	7,10,18	4,11,15,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	7,10,16,17	4,11,15,17	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	7,10,14,17,18	4,11,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	7,10,14,16	4,11	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	7,10,14,17	4,11,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	7,10,14,16,18	4,11,15,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	7,10,18	4,11,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	7,10,16,17	4,11,13,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	7,10	4,11,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	7,10,16,17,18	4,11,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	7,10,14,17	4,11,13,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	7,10,14,16,18	4,11,13,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	7,10,14,17,18	4,11,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	7,10,14,16	4,11,13,15	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	7,10,12,17,18	4,11,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	7,10,12,16	4,11	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	7,10,12,17	4,11,15,17	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	7,10,12,16,18	4,11,15,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	7,10,12,14	4,11	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	7,10,12,14,16,17,18	4,11,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	7,10,12,14,18	4,11,15,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	7,10,12,14,16,17	4,11,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	7,10,12,17	4,11,13,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	7,10,12,16,18	4,11,13,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	7,10,12,17,18	4,11,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	7,10,12,16	4,11,13,15	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	7,10,12,14,18	4,11,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	7,10,12,14,16,17	4,11,13,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	7,10,12,14	4,11,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	7,10,12,14,16,17,18	4,11,13,15,17,18	2^{-12}

Table 0.149 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,1,0,0,1,0,1,0,0,0,0,0,0,0) \xrightarrow{1r} (1,0,0,0,0,0,1,0,0,0,1,0,1,1,1,1)$	7,17,18	4,9,17,18	2^{-12}
$(0,0,0,1,0,0,1,0,1,0,0,0,0,0,0,1) \xrightarrow{1r} (0,1,1,1,1,0,1,1,1,0,1,0,0,0,0,1)$	7,16	4,9	$2^{-17.5}$
$(0,0,0,1,0,0,1,0,1,0,0,0,0,0,1,0) \xrightarrow{1r} (0,1,0,0,0,0,1,1,0,0,1,0,1,1,1,1)$	7,17	4,9,15,17	2^{-12}
$(0,0,0,1,0,0,1,0,1,0,0,0,0,0,1,1) \xrightarrow{1r} (1,0,1,1,1,1,0,0,1,1,0,1,0,0,0,1)$	7,16,18	4,9,15,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,0,1,0,0,0,0,1,0,0) \xrightarrow{1r} (0,1,0,1,1,1,1,1,0,1,0,1,0,0,0,0)$	7,14	4,9	$2^{-17.5}$
$(0,0,0,1,0,0,1,0,1,0,0,0,0,1,0,1) \xrightarrow{1r} (1,0,1,0,0,0,0,0,1,0,1,0,1,1,1,0)$	7,14,16,17,18	4,9,17,18	2^{-23}
$(0,0,0,1,0,0,1,0,1,0,0,0,0,1,1,0) \xrightarrow{1r} (1,0,0,1,1,1,1,0,0,1,0,1,0,0,0,0)$	7,14,18	4,9,15,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,0,1,0,0,0,0,1,1,1) \xrightarrow{1r} (0,1,1,0,0,0,0,1,1,0,1,0,1,1,1,0)$	7,14,16,17	4,9,15,17	2^{-23}
$(0,0,0,1,0,0,1,0,1,0,0,0,1,0,0,0) \xrightarrow{1r} (0,1,0,1,0,1,1,0,0,1,1,0,1,1,1,1)$	7,17	4,9,13,17	$2^{-17.5}$
$(0,0,0,1,0,0,1,0,1,0,0,0,1,0,0,1) \xrightarrow{1r} (1,0,1,0,1,0,0,1,1,0,0,1,0,0,0,1)$	7,16,18	4,9,13,18	2^{-23}
$(0,0,0,1,0,0,1,0,1,0,0,0,1,0,1,0) \xrightarrow{1r} (1,0,0,1,0,1,1,1,0,1,1,0,1,1,1,1)$	7,17,18	4,9,13,15,17,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,0,1,0,0,0,1,0,1,1) \xrightarrow{1r} (0,1,1,0,1,0,0,0,1,0,0,1,0,0,0,1)$	7,16	4,9,13,15	2^{-23}
$(0,0,0,1,0,0,1,0,1,0,0,0,1,1,0,0) \xrightarrow{1r} (1,0,0,0,1,0,1,1,0,0,0,1,0,0,0,0)$	7,14,18	4,9,13,18	2^{-12}
$(0,0,0,1,0,0,1,0,1,0,0,0,1,1,0,1) \xrightarrow{1r} (0,1,1,1,0,1,0,0,1,1,1,0,1,1,1,0)$	7,14,16,17	4,9,13,17	$2^{-17.5}$
$(0,0,0,1,0,0,1,0,1,0,0,0,1,1,1,0) \xrightarrow{1r} (0,1,0,0,1,0,1,0,0,0,0,1,0,0,0,0)$	7,14	4,9,13,15	2^{-12}
$(0,0,0,1,0,0,1,0,1,0,0,0,1,1,1,1) \xrightarrow{1r} (1,0,1,1,0,1,0,1,1,1,1,0,1,1,1,0)$	7,14,16,17,18	4,9,13,15,17,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,0,1,0,0,1,0,0,0,0) \xrightarrow{1r} (0,1,0,1,1,1,0,1,0,1,1,1,0,0,0,0)$	7,12	4,9	$2^{-17.5}$
$(0,0,0,1,0,0,1,0,1,0,0,1,0,0,0,1) \xrightarrow{1r} (1,0,1,0,0,0,1,0,1,0,0,0,1,1,1,0)$	7,12,16,17,18	4,9,17,18	2^{-34}
$(0,0,0,1,0,0,1,0,1,0,0,1,0,0,1,0) \xrightarrow{1r} (1,0,0,1,1,1,0,0,0,1,1,1,0,0,0,0)$	7,12,18	4,9,15,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,0,1,0,0,1,0,0,1,1) \xrightarrow{1r} (0,1,1,0,0,0,1,1,1,0,0,0,1,1,1,0)$	7,12,16,17	4,9,15,17	2^{-34}
$(0,0,0,1,0,0,1,0,1,0,0,1,0,1,0,0) \xrightarrow{1r} (1,0,0,0,0,0,0,0,0,0,0,0,1,1,1,1)$	7,12,14,17,18	4,9,17,18	2^{-23}
$(0,0,0,1,0,0,1,0,1,0,0,1,0,1,0,1) \xrightarrow{1r} (0,1,1,1,1,1,1,1,1,1,1,0,0,0,1)$	7,12,14,16	4,9	$2^{-17.5}$
$(0,0,0,1,0,0,1,0,1,0,0,1,0,1,1,0) \xrightarrow{1r} (0,1,0,0,0,0,0,1,0,0,0,0,1,1,1,1)$	7,12,14,17	4,9,15,17	2^{-23}
$(0,0,0,1,0,0,1,0,1,0,0,1,0,1,1,1) \xrightarrow{1r} (1,0,1,1,1,1,1,0,1,1,1,1,0,0,0,1)$	7,12,14,16,18	4,9,15,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,0,1,0,0,1,1,0,0,0) \xrightarrow{1r} (1,0,0,0,1,0,0,1,0,0,1,1,0,0,0,0)$	7,12,18	4,9,13,18	2^{-12}
$(0,0,0,1,0,0,1,0,1,0,0,1,1,0,0,1) \xrightarrow{1r} (0,1,1,1,0,1,1,0,1,1,0,0,1,1,1,0)$	7,12,16,17	4,9,13,17	$2^{-28.5}$
$(0,0,0,1,0,0,1,0,1,0,0,1,1,0,1,0) \xrightarrow{1r} (0,1,0,0,1,0,0,0,0,0,1,1,0,0,0,0)$	7,12	4,9,13,15	2^{-12}
$(0,0,0,1,0,0,1,0,1,0,0,1,1,0,1,1) \xrightarrow{1r} (1,0,1,1,0,1,1,1,1,1,0,0,1,1,1,0)$	7,12,16,17,18	4,9,13,15,17,18	$2^{-28.5}$
$(0,0,0,1,0,0,1,0,1,0,0,1,1,1,0,0) \xrightarrow{1r} (0,1,0,1,0,1,0,0,0,1,0,0,1,1,1,1)$	7,12,14,17	4,9,13,17	$2^{-28.5}$
$(0,0,0,1,0,0,1,0,1,0,0,1,1,1,0,1) \xrightarrow{1r} (1,0,1,0,1,0,1,1,1,0,1,1,0,0,0,1)$	7,12,14,16,18	4,9,13,18	2^{-23}
$(0,0,0,1,0,0,1,0,1,0,0,1,1,1,1,0) \xrightarrow{1r} (1,0,0,1,0,1,0,1,0,1,0,0,1,1,1,1)$	7,12,14,17,18	4,9,13,15,17,18	$2^{-28.5}$
$(0,0,0,1,0,0,1,0,1,0,0,1,1,1,1,1) \xrightarrow{1r} (0,1,1,0,1,0,1,0,1,0,1,1,0,0,0,1)$	7,12,14,16	4,9,13,15	2^{-23}

Table 0.150 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	7,17	4,9,11,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	7,16,18	4,9,11,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	7,17,18	4,9,11,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	7,16	4,9,11,15	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	7,14,18	4,9,11,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	7,14,16,17	4,9,11,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	7,14	4,9,11,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	7,14,16,17,18	4,9,11,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	7,17,18	4,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	7,16	4,9,11,13	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	7,17	4,9,11,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	7,16,18	4,9,11,13,15,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	7,14	4,9,11,13	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	7,14,16,17,18	4,9,11,13,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	7,14,18	4,9,11,13,15,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	7,14,16,17	4,9,11,13,15,17	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	7,12,18	4,9,11,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	7,12,16,17	4,9,11,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	7,12	4,9,11,15	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	7,12,16,17,18	4,9,11,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	7,12,14,17	4,9,11,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	7,12,14,16,18	4,9,11,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	7,12,14,17,18	4,9,11,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	7,12,14,16	4,9,11,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	7,12	4,9,11,13	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	7,12,16,17,18	4,9,11,13,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	7,12,18	4,9,11,13,15,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	7,12,16,17	4,9,11,13,15,17	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	7,12,14,17,18	4,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	7,12,14,16	4,9,11,13	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	7,12,14,17	4,9,11,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	7,12,14,16,18	4,9,11,13,15,18	2^{-12}

Table 0.151 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	7,10	4,9	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	7,10,16,17,18	4,9,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	7,10,18	4,9,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	7,10,16,17	4,9,15,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	7,10,14,17,18	4,9,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	7,10,14,16	4,9	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	7,10,14,17	4,9,15,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	7,10,14,16,18	4,9,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	7,10,18	4,9,13,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	7,10,16,17	4,9,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	7,10	4,9,13,15	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	7,10,16,17,18	4,9,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	7,10,14,17	4,9,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	7,10,14,16,18	4,9,13,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	7,10,14,17,18	4,9,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	7,10,14,16	4,9,13,15	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	7,10,12,17,18	4,9,17,18	2^{-1}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	7,10,12,16	4,9	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	7,10,12,17	4,9,15,17	2^{-1}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	7,10,12,16,18	4,9,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	7,10,12,14	4,9	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	7,10,12,14,16,17,18	4,9,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	7,10,12,14,18	4,9,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	7,10,12,14,16,17	4,9,15,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	7,10,12,17	4,9,13,17	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	7,10,12,16,18	4,9,13,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	7,10,12,17,18	4,9,13,15,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	7,10,12,16	4,9,13,15	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	7,10,12,14,18	4,9,13,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	7,10,12,14,16,17	4,9,13,17	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	7,10,12,14	4,9,13,15	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	7,10,12,14,16,17,18	4,9,13,15,17,18	$2^{-6.5}$

Table 0.152 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	7,10,18	4,9,11,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	7,10,16,17	4,9,11,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	7,10	4,9,11,15	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	7,10,16,17,18	4,9,11,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	7,10,14,17	4,9,11,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	7,10,14,16,18	4,9,11,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	7,10,14,17,18	4,9,11,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	7,10,14,16	4,9,11,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	7,10	4,9,11,13	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	7,10,16,17,18	4,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	7,10,18	4,9,11,13,15,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	7,10,16,17	4,9,11,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	7,10,14,17,18	4,9,11,13,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	7,10,14,16	4,9,11,13	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	7,10,14,17	4,9,11,13,15,17	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	7,10,14,16,18	4,9,11,13,15,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	7,10,12,17	4,9,11,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	7,10,12,16,18	4,9,11,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	7,10,12,17,18	4,9,11,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	7,10,12,16	4,9,11,15	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	7,10,12,14,18	4,9,11,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	7,10,12,14,16,17	4,9,11,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	7,10,12,14	4,9,11,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	7,10,12,14,16,17,18	4,9,11,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	7,10,12,17,18	4,9,11,13,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	7,10,12,16	4,9,11,13	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	7,10,12,17	4,9,11,13,15,17	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	7,10,12,16,18	4,9,11,13,15,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	7,10,12,14	4,9,11,13	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	7,10,12,14,16,17,18	4,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	7,10,12,14,18	4,9,11,13,15,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	7,10,12,14,16,17	4,9,11,13,15,17	$2^{-17.5}$

Table 0.153 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	7,18	4,8,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	7,16,17	4,8,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	7	4,8,15	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	7,16,17,18	4,8,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	7,14,17	4,8,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	7,14,16,18	4,8,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	7,14,17,18	4,8,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	7,14,16	4,8,15	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	7	4,8,13	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	7,16,17,18	4,8,13,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	7,18	4,8,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	7,16,17	4,8,13,15,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	7,14,17,18	4,8,13,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	7,14,16	4,8,13	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	7,14,17	4,8,13,15,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	7,14,16,18	4,8,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	7,12,17	4,8,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	7,12,16,18	4,8,18	2^{-1}
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	7,12,17,18	4,8,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	7,12,16	4,8,15	2^{-1}
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	7,12,14,18	4,8,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	7,12,14,16,17	4,8,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	7,12,14	4,8,15	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	7,12,14,16,17,18	4,8,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	7,12,17,18	4,8,13,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	7,12,16	4,8,13	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	7,12,17	4,8,13,15,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	7,12,16,18	4,8,13,15,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	7,12,14	4,8,13	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	7,12,14,16,17,18	4,8,13,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	7,12,14,18	4,8,13,15,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	7,12,14,16,17	4,8,13,15,17	2^{-12}

Table 0.154 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	7	4,8,11	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	7,16,17,18	4,8,11,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	7,18	4,8,11,15,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	7,16,17	4,8,11,15,17	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	7,14,17,18	4,8,11,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	7,14,16	4,8,11	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	7,14,17	4,8,11,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	7,14,16,18	4,8,11,15,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	7,18	4,8,11,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	7,16,17	4,8,11,13,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	7	4,8,11,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	7,16,17,18	4,8,11,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	7,14,17	4,8,11,13,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	7,14,16,18	4,8,11,13,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	7,14,17,18	4,8,11,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	7,14,16	4,8,11,13,15	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	7,12,17,18	4,8,11,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	7,12,16	4,8,11	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	7,12,17	4,8,11,15,17	$2^{-28.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	7,12,16,18	4,8,11,15,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	7,12,14	4,8,11	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	7,12,14,16,17,18	4,8,11,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	7,12,14,18	4,8,11,15,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	7,12,14,16,17	4,8,11,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	7,12,17	4,8,11,13,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	7,12,16,18	4,8,11,13,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	7,12,17,18	4,8,11,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	7,12,16	4,8,11,13,15	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	7,12,14,18	4,8,11,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	7,12,14,16,17	4,8,11,13,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	7,12,14	4,8,11,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	7,12,14,16,17,18	4,8,11,13,15,17,18	2^{-23}

Table 0.155 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(2)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,1,0,0,1,1,0,1,0,0,0,0,0,0) \xrightarrow{1r} (0,0,0,1,1,1,0,1,1,1,0,1,0,0,0,1)$	7,10,17	4,8,17	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,0,1,0,0,0,0,0,1) \xrightarrow{1r} (1,1,1,0,0,0,1,0,0,0,1,0,1,1,1,1)$	7,10,16,18	4,8,18	2^{-12}
$(0,0,0,1,0,0,1,1,0,1,0,0,0,0,1,0) \xrightarrow{1r} (1,1,0,1,1,1,0,0,1,1,0,1,0,0,0,1)$	7,10,17,18	4,8,15,17,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,0,1,0,0,0,0,1,1) \xrightarrow{1r} (0,0,1,0,0,0,1,1,0,0,1,0,1,1,1,1)$	7,10,16	4,8,15	2^{-12}
$(0,0,0,1,0,0,1,1,0,1,0,0,0,1,0,0) \xrightarrow{1r} (1,1,0,0,0,0,0,0,1,0,1,0,1,1,1,0)$	7,10,14,18	4,8,18	2^{-23}
$(0,0,0,1,0,0,1,1,0,1,0,0,0,1,0,1) \xrightarrow{1r} (0,0,1,1,1,1,1,1,0,1,0,1,0,0,0,0)$	7,10,14,16,17	4,8,17	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,0,1,0,0,0,1,1,0) \xrightarrow{1r} (0,0,0,0,0,0,0,0,1,1,0,1,0,1,1,1,0)$	7,10,14	4,8,15	2^{-23}
$(0,0,0,1,0,0,1,1,0,1,0,0,0,1,1,1) \xrightarrow{1r} (1,1,1,1,1,1,1,0,0,1,0,1,0,0,0,0)$	7,10,14,16,17,18	4,8,15,17,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,0,1,0,0,1,0,0,0) \xrightarrow{1r} (1,1,0,0,1,0,0,1,1,0,0,1,0,0,0,1)$	7,10,17,18	4,8,13,17,18	2^{-23}
$(0,0,0,1,0,0,1,1,0,1,0,0,1,0,0,1) \xrightarrow{1r} (0,0,1,1,0,1,1,0,0,1,1,0,1,1,1,1)$	7,10,16	4,8,13	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,0,1,0,0,1,0,1,0) \xrightarrow{1r} (0,0,0,0,1,0,0,0,1,0,0,1,0,0,0,1)$	7,10,17	4,8,13,15,17	2^{-23}
$(0,0,0,1,0,0,1,1,0,1,0,0,1,0,1,1) \xrightarrow{1r} (1,1,1,1,0,1,1,1,0,1,1,0,1,1,1,1)$	7,10,16,18	4,8,13,15,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,0,1,0,0,1,1,0,0) \xrightarrow{1r} (0,0,0,1,0,1,0,0,1,1,1,0,1,1,1,0)$	7,10,14	4,8,13	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,0,1,0,0,1,1,0,1) \xrightarrow{1r} (1,1,1,0,1,0,1,1,0,0,0,1,0,0,0,0)$	7,10,14,16,17,18	4,8,13,17,18	2^{-12}
$(0,0,0,1,0,0,1,1,0,1,0,0,1,1,1,0) \xrightarrow{1r} (1,1,0,1,0,1,0,1,1,1,1,0,1,1,1,0)$	7,10,14,18	4,8,13,15,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,0,1,0,0,1,1,1,1) \xrightarrow{1r} (0,0,1,0,1,0,1,0,0,0,0,1,0,0,0,0)$	7,10,14,16,17	4,8,13,15,17	2^{-12}
$(0,0,0,1,0,0,1,1,0,1,0,1,0,0,0,0) \xrightarrow{1r} (1,1,0,0,0,0,1,0,1,0,0,0,1,1,1,0)$	7,10,12,18	4,8,18	2^{-34}
$(0,0,0,1,0,0,1,1,0,1,0,1,0,0,0,1) \xrightarrow{1r} (0,0,1,1,1,1,0,1,0,1,1,1,0,0,0,0)$	7,10,12,16,17	4,8,17	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,0,1,0,1,0,0,1,0) \xrightarrow{1r} (0,0,0,0,0,0,1,1,1,0,0,0,1,1,1,0)$	7,10,12	4,8,15	2^{-34}
$(0,0,0,1,0,0,1,1,0,1,0,1,0,0,1,1) \xrightarrow{1r} (1,1,1,1,1,1,0,0,0,1,1,1,0,0,0,0)$	7,10,12,16,17,18	4,8,15,17,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,0,1,0,1,0,1,0,0) \xrightarrow{1r} (0,0,0,1,1,1,1,1,1,1,1,0,0,0,1)$	7,10,12,14,17	4,8,17	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,0,1,0,1,0,1,0,1) \xrightarrow{1r} (1,1,1,0,0,0,0,0,0,0,0,0,1,1,1,1)$	7,10,12,14,16,18	4,8,18	2^{-23}
$(0,0,0,1,0,0,1,1,0,1,0,1,0,1,1,0) \xrightarrow{1r} (1,1,0,1,1,1,1,0,1,1,1,1,0,0,0,1)$	7,10,12,14,17,18	4,8,15,17,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,0,1,0,1,0,1,1,1) \xrightarrow{1r} (0,0,1,0,0,0,0,1,0,0,0,0,1,1,1,1)$	7,10,12,14,16	4,8,15	2^{-23}
$(0,0,0,1,0,0,1,1,0,1,0,1,0,1,0,0) \xrightarrow{1r} (0,0,0,1,0,1,1,0,1,1,0,0,1,1,1,0)$	7,10,12	4,8,13	$2^{-28.5}$
$(0,0,0,1,0,0,1,1,0,1,0,1,1,0,0,1) \xrightarrow{1r} (1,1,1,0,1,0,0,1,0,0,1,1,0,0,0,0)$	7,10,12,16,17,18	4,8,13,17,18	2^{-12}
$(0,0,0,1,0,0,1,1,0,1,0,1,1,0,1,0) \xrightarrow{1r} (1,1,0,1,0,1,1,1,1,1,0,0,1,1,1,0)$	7,10,12,18	4,8,13,15,18	$2^{-28.5}$
$(0,0,0,1,0,0,1,1,0,1,0,1,1,0,1,1) \xrightarrow{1r} (0,0,1,0,1,0,0,0,0,0,1,1,0,0,0,0)$	7,10,12,16,17	4,8,13,15,17	2^{-12}
$(0,0,0,1,0,0,1,1,0,1,0,1,1,1,0,0) \xrightarrow{1r} (1,1,0,0,1,0,1,1,1,0,1,1,0,0,0,1)$	7,10,12,14,17,18	4,8,13,17,18	2^{-23}
$(0,0,0,1,0,0,1,1,0,1,0,1,1,1,0,1) \xrightarrow{1r} (0,0,1,1,0,1,0,0,0,1,0,0,1,1,1,1)$	7,10,12,14,16	4,8,13	$2^{-28.5}$
$(0,0,0,1,0,0,1,1,0,1,0,1,1,1,1,0) \xrightarrow{1r} (0,0,0,0,1,0,1,0,1,0,1,1,0,0,0,1)$	7,10,12,14,17	4,8,13,15,17	2^{-23}
$(0,0,0,1,0,0,1,1,0,1,0,1,1,1,1,1) \xrightarrow{1r} (1,1,1,1,0,1,0,1,0,1,0,1,0,1,1,1)$	7,10,12,14,16,18	4,8,13,15,18	$2^{-28.5}$

Table 0.156 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,1,0,0,1,1,0,1,1,0,0,0,0,0) \xrightarrow{1r} (1,1,0,1,1,0,0,1,1,0,0,0,0,0,0,1)$	7,10,17,18	4,8,11,17,18	$2^{-28.5}$
$(0,0,0,1,0,0,1,1,0,1,1,0,0,0,0,1) \xrightarrow{1r} (0,0,1,0,0,1,1,0,0,1,1,1,1,1,1,1)$	7,10,16	4,8,11	2^{-23}
$(0,0,0,1,0,0,1,1,0,1,1,0,0,0,1,0) \xrightarrow{1r} (0,0,0,1,1,0,0,0,1,0,0,0,0,0,0,1)$	7,10,17	4,8,11,15,17	$2^{-28.5}$
$(0,0,0,1,0,0,1,1,0,1,1,0,0,0,1,1) \xrightarrow{1r} (1,1,1,0,0,1,1,1,0,1,1,1,1,1,1,1)$	7,10,16,18	4,8,11,15,18	2^{-23}
$(0,0,0,1,0,0,1,1,0,1,1,0,0,1,0,0) \xrightarrow{1r} (0,0,0,0,0,1,0,0,1,1,1,1,1,1,1,0)$	7,10,14	4,8,11	2^{-23}
$(0,0,0,1,0,0,1,1,0,1,1,0,0,1,0,1) \xrightarrow{1r} (1,1,1,1,0,1,1,0,0,0,0,0,0,0,0,0)$	7,10,14,16,17,18	4,8,11,17,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,0,1,1,0,0,1,1,0) \xrightarrow{1r} (1,1,0,0,0,1,0,1,1,1,1,1,1,1,1,0)$	7,10,14,18	4,8,11,15,18	2^{-23}
$(0,0,0,1,0,0,1,1,0,1,1,0,0,1,1,1) \xrightarrow{1r} (0,0,1,1,1,0,1,0,0,0,0,0,0,0,0,0)$	7,10,14,16,17	4,8,11,15,17	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,0,1,1,0,1,0,0,0) \xrightarrow{1r} (0,0,0,0,1,1,0,1,1,1,0,0,0,0,0,1)$	7,10,17	4,8,11,13,17	2^{-23}
$(0,0,0,1,0,0,1,1,0,1,1,0,1,0,0,1) \xrightarrow{1r} (1,1,1,1,0,0,1,0,0,0,1,1,1,1,1,1)$	7,10,16,18	4,8,11,13,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,0,1,1,0,1,0,1,0) \xrightarrow{1r} (1,1,0,0,1,1,0,0,1,1,0,0,0,0,0,1)$	7,10,17,18	4,8,11,13,15,17,18	2^{-23}
$(0,0,0,1,0,0,1,1,0,1,1,0,1,0,1,1) \xrightarrow{1r} (0,0,1,1,0,0,1,1,0,0,1,1,1,1,1,1)$	7,10,16	4,8,11,13,15	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,0,1,1,0,1,1,0,0) \xrightarrow{1r} (1,1,0,1,0,0,0,0,1,0,1,1,1,1,1,0)$	7,10,14,18	4,8,11,13,18	$2^{-28.5}$
$(0,0,0,1,0,0,1,1,0,1,1,0,1,1,0,1) \xrightarrow{1r} (0,0,1,0,1,1,1,1,0,1,0,0,0,0,0,0)$	7,10,14,16,17	4,8,11,13,17	2^{-23}
$(0,0,0,1,0,0,1,1,0,1,1,0,1,1,1,0) \xrightarrow{1r} (0,0,0,1,0,0,0,1,1,0,1,1,1,1,1,0)$	7,10,14	4,8,11,13,15	$2^{-28.5}$
$(0,0,0,1,0,0,1,1,0,1,1,0,1,1,1,1) \xrightarrow{1r} (1,1,1,0,1,1,1,0,0,1,0,0,0,0,0,0)$	7,10,14,16,17,18	4,8,11,13,15,17,18	2^{-23}
$(0,0,0,1,0,0,1,1,0,1,1,1,0,0,0,0) \xrightarrow{1r} (0,0,0,0,0,1,1,0,1,1,0,1,1,1,1,0)$	7,10,12	4,8,11	2^{-23}
$(0,0,0,1,0,0,1,1,0,1,1,1,0,0,0,1) \xrightarrow{1r} (1,1,1,1,0,0,1,0,0,1,0,0,0,0,0,0)$	7,10,12,16,17,18	4,8,11,17,18	$2^{-6.5}$
$(0,0,0,1,0,0,1,1,0,1,1,1,0,0,1,0) \xrightarrow{1r} (1,1,0,0,0,1,1,1,1,0,1,1,1,1,1,0)$	7,10,12,18	4,8,11,15,18	2^{-23}
$(0,0,0,1,0,0,1,1,0,1,1,1,0,0,1,1) \xrightarrow{1r} (0,0,1,1,1,0,0,0,0,0,1,0,0,0,0,0)$	7,10,12,16,17	4,8,11,15,17	$2^{-6.5}$
$(0,0,0,1,0,0,1,1,0,1,1,1,0,1,0,0) \xrightarrow{1r} (1,1,0,1,1,0,1,1,1,0,1,0,0,0,0,1)$	7,10,12,14,17,18	4,8,11,17,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,0,1,1,1,0,1,0,1) \xrightarrow{1r} (0,0,1,0,0,1,0,0,0,1,0,1,1,1,1,1)$	7,10,12,14,16	4,8,11	2^{-23}
$(0,0,0,1,0,0,1,1,0,1,1,1,0,1,1,0) \xrightarrow{1r} (0,0,0,1,1,0,1,0,1,0,1,0,0,0,0,1)$	7,10,12,14,17	4,8,11,15,17	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,0,1,1,1,0,1,1,1) \xrightarrow{1r} (1,1,1,0,0,1,0,1,0,1,0,1,0,1,1,1)$	7,10,12,14,16,18	4,8,11,15,18	2^{-23}
$(0,0,0,1,0,0,1,1,0,1,1,1,1,0,0,0) \xrightarrow{1r} (1,1,0,1,0,0,1,0,1,0,0,1,1,1,1,0)$	7,10,12,18	4,8,11,13,18	$2^{-28.5}$
$(0,0,0,1,0,0,1,1,0,1,1,1,1,0,0,1) \xrightarrow{1r} (0,0,1,0,1,1,0,1,0,1,1,0,0,0,0,0)$	7,10,12,16,17	4,8,11,13,17	2^{-12}
$(0,0,0,1,0,0,1,1,0,1,1,1,1,0,1,0) \xrightarrow{1r} (0,0,0,1,0,0,1,1,1,0,0,1,1,1,1,0)$	7,10,12	4,8,11,13,15	$2^{-28.5}$
$(0,0,0,1,0,0,1,1,0,1,1,1,1,0,1,1) \xrightarrow{1r} (1,1,1,0,1,1,0,0,0,1,1,0,0,0,0,0)$	7,10,12,16,17,18	4,8,11,13,15,17,18	2^{-12}
$(0,0,0,1,0,0,1,1,0,1,1,1,1,1,0,0) \xrightarrow{1r} (0,0,0,0,1,1,1,1,1,1,1,0,0,0,0,1)$	7,10,12,14,17	4,8,11,13,17	2^{-12}
$(0,0,0,1,0,0,1,1,0,1,1,1,1,1,0,1) \xrightarrow{1r} (1,1,1,1,0,0,0,0,0,0,0,0,1,1,1,1)$	7,10,12,14,16,18	4,8,11,13,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,0,1,1,1,1,1,1,0) \xrightarrow{1r} (1,1,0,0,1,1,1,0,1,1,1,0,0,0,0,1)$	7,10,12,14,17,18	4,8,11,13,15,17,18	2^{-12}
$(0,0,0,1,0,0,1,1,0,1,1,1,1,1,1,1) \xrightarrow{1r} (0,0,1,1,0,0,0,1,0,0,0,1,1,1,1,1)$	7,10,12,14,16	4,8,11,13,15	$2^{-17.5}$

Table 0.157 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,1,0,0,1,1,1,0,0,0,0,0,0,0) \xrightarrow{1r} (0,1,1,1,1,0,1,1,1,0,1,0,0,1,0,0)$	7	4,8,9	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,1,0,0,0,0,0,0,1) \xrightarrow{1r} (1,0,0,0,0,0,1,0,0,0,1,0,1,1,0,0)$	7,16,17,18	4,8,9,17,18	2^{-12}
$(0,0,0,1,0,0,1,1,1,0,0,0,0,0,1,0) \xrightarrow{1r} (1,0,1,1,1,0,0,1,1,0,1,0,0,1,0,0)$	7,18	4,8,9,15,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,1,0,0,0,0,0,1,1) \xrightarrow{1r} (0,1,0,0,0,0,1,1,0,0,1,0,1,1,0,0)$	7,16,17	4,8,9,15,17	2^{-12}
$(0,0,0,1,0,0,1,1,1,0,0,0,0,1,0,0) \xrightarrow{1r} (1,0,1,0,0,0,0,0,1,0,1,0,1,1,0,1)$	7,14,17,18	4,8,9,17,18	2^{-23}
$(0,0,0,1,0,0,1,1,1,0,0,0,0,1,0,1) \xrightarrow{1r} (0,1,0,1,1,1,1,1,0,1,0,1,0,0,1,1)$	7,14,16	4,8,9	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,1,0,0,0,0,1,1,0) \xrightarrow{1r} (0,1,1,0,0,0,0,1,1,0,1,0,1,1,0,1)$	7,14,17	4,8,9,15,17	2^{-23}
$(0,0,0,1,0,0,1,1,1,0,0,0,0,1,1,1) \xrightarrow{1r} (1,0,0,1,1,1,1,0,0,1,0,1,0,0,1,1)$	7,14,16,18	4,8,9,15,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,1,0,0,0,1,0,0,0) \xrightarrow{1r} (1,0,1,0,1,0,0,1,1,0,0,1,0,0,1,0)$	7,18	4,8,9,13,18	2^{-23}
$(0,0,0,1,0,0,1,1,1,0,0,0,1,0,0,1) \xrightarrow{1r} (0,1,0,1,0,1,1,0,0,1,1,0,1,1,0,0)$	7,16,17	4,8,9,13,17	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,1,0,0,0,1,0,1,0) \xrightarrow{1r} (0,1,1,0,1,0,0,0,1,0,0,1,0,0,1,0)$	7	4,8,9,13,15	2^{-23}
$(0,0,0,1,0,0,1,1,1,0,0,0,1,0,1,1) \xrightarrow{1r} (1,0,0,1,0,1,1,1,0,1,1,0,1,1,0,0)$	7,16,17,18	4,8,9,13,15,17,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,1,0,0,0,1,1,0,0) \xrightarrow{1r} (0,1,1,1,0,1,0,0,1,1,1,0,1,1,0,1)$	7,14,17	4,8,9,13,17	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,1,0,0,0,1,1,0,1) \xrightarrow{1r} (1,0,0,0,1,0,1,1,0,0,0,1,0,0,1,1)$	7,14,16,18	4,8,9,13,18	2^{-12}
$(0,0,0,1,0,0,1,1,1,0,0,0,1,1,1,0) \xrightarrow{1r} (1,0,1,1,0,1,0,1,1,1,1,0,1,1,0,1)$	7,14,17,18	4,8,9,13,15,17,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,1,0,0,0,1,1,1,1) \xrightarrow{1r} (0,1,0,0,1,0,1,0,0,0,0,1,0,0,1,1)$	7,14,16	4,8,9,13,15	2^{-12}
$(0,0,0,1,0,0,1,1,1,0,0,1,0,0,0,0) \xrightarrow{1r} (1,0,1,0,0,0,1,0,1,0,0,0,1,1,0,1)$	7,12,17,18	4,8,9,17,18	2^{-34}
$(0,0,0,1,0,0,1,1,1,0,0,1,0,0,0,1) \xrightarrow{1r} (0,1,0,1,1,1,0,1,0,1,1,1,0,0,1,1)$	7,12,16	4,8,9	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,1,0,0,1,0,0,1,0) \xrightarrow{1r} (0,1,1,0,0,0,1,1,1,0,0,0,1,1,0,1)$	7,12,17	4,8,9,15,17	2^{-34}
$(0,0,0,1,0,0,1,1,1,0,0,1,0,0,1,1) \xrightarrow{1r} (1,0,0,1,1,1,0,0,0,1,1,1,0,0,1,1)$	7,12,16,18	4,8,9,15,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,1,0,0,1,0,1,0,0) \xrightarrow{1r} (0,1,1,1,1,1,1,1,1,1,1,0,0,1,0)$	7,12,14	4,8,9	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,1,0,0,1,0,1,0,1) \xrightarrow{1r} (1,0,0,0,0,0,0,0,0,0,0,0,1,1,0,0)$	7,12,14,16,17,18	4,8,9,17,18	2^{-23}
$(0,0,0,1,0,0,1,1,1,0,0,1,0,1,1,0) \xrightarrow{1r} (1,0,1,1,1,1,1,0,1,1,1,1,0,0,1,0)$	7,12,14,18	4,8,9,15,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,1,0,0,1,0,1,1,1) \xrightarrow{1r} (0,1,0,0,0,0,0,1,0,0,0,0,1,1,0,0)$	7,12,14,16,17	4,8,9,15,17	2^{-23}
$(0,0,0,1,0,0,1,1,1,0,0,1,1,0,0,0) \xrightarrow{1r} (0,1,1,1,0,1,1,0,1,1,1,0,0,1,1,0,1)$	7,12,17	4,8,9,13,17	$2^{-28.5}$
$(0,0,0,1,0,0,1,1,1,0,0,1,1,0,0,1) \xrightarrow{1r} (1,0,0,0,1,0,0,1,0,0,1,1,0,0,1,1)$	7,12,16,18	4,8,9,13,18	2^{-12}
$(0,0,0,1,0,0,1,1,1,0,0,1,1,0,1,0) \xrightarrow{1r} (1,0,1,1,0,1,1,1,1,1,0,0,1,1,0,1)$	7,12,17,18	4,8,9,13,15,17,18	$2^{-28.5}$
$(0,0,0,1,0,0,1,1,1,0,0,1,1,0,1,1) \xrightarrow{1r} (0,1,0,0,1,0,0,0,0,0,1,1,0,0,1,1)$	7,12,16	4,8,9,13,15	2^{-12}
$(0,0,0,1,0,0,1,1,1,0,0,1,1,1,0,0) \xrightarrow{1r} (1,0,1,0,1,0,1,1,1,0,1,1,0,0,1,0)$	7,12,14,18	4,8,9,13,18	2^{-23}
$(0,0,0,1,0,0,1,1,1,0,0,1,1,1,0,1) \xrightarrow{1r} (0,1,0,1,0,1,0,0,0,1,0,0,1,1,0,0)$	7,12,14,16,17	4,8,9,13,17	$2^{-28.5}$
$(0,0,0,1,0,0,1,1,1,0,0,1,1,1,1,0) \xrightarrow{1r} (0,1,1,0,1,0,1,0,1,0,1,0,1,1,0,0,1,0)$	7,12,14	4,8,9,13,15	2^{-23}
$(0,0,0,1,0,0,1,1,1,0,0,1,1,1,1,1) \xrightarrow{1r} (1,0,0,1,0,1,0,1,0,1,0,1,0,0,1,1,0,0)$	7,12,14,16,17,18	4,8,9,13,15,17,18	$2^{-28.5}$

Table 0.158 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,1,0,0,1,1,1,0,1,0,0,0,0,0) \xrightarrow{1r} (1,0,1,1,1,0,0,1,1,0,0,0,0,0,1,0)$	7,18	4,8,9,11,18	$2^{-28.5}$
$(0,0,0,1,0,0,1,1,1,0,1,0,0,0,0,1) \xrightarrow{1r} (0,1,0,0,0,1,1,0,0,1,1,1,1,1,0,0)$	7,16,17	4,8,9,11,17	2^{-23}
$(0,0,0,1,0,0,1,1,1,0,1,0,0,0,1,0) \xrightarrow{1r} (0,1,1,1,1,0,0,0,1,0,0,0,0,0,1,0)$	7	4,8,9,11,15	$2^{-28.5}$
$(0,0,0,1,0,0,1,1,1,0,1,0,0,0,1,1) \xrightarrow{1r} (1,0,0,0,0,1,1,1,0,1,1,1,1,1,0,0)$	7,16,17,18	4,8,9,11,15,17,18	2^{-23}
$(0,0,0,1,0,0,1,1,1,0,1,0,0,1,0,0) \xrightarrow{1r} (0,1,1,0,0,1,0,0,1,1,1,1,1,1,0,1)$	7,14,17	4,8,9,11,17	2^{-23}
$(0,0,0,1,0,0,1,1,1,0,1,0,0,1,0,1) \xrightarrow{1r} (1,0,0,1,1,0,1,1,0,0,0,0,0,0,1,1)$	7,14,16,18	4,8,9,11,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,1,0,1,0,0,1,1,0) \xrightarrow{1r} (1,0,1,0,0,1,0,1,1,1,1,1,1,1,0,1)$	7,14,17,18	4,8,9,11,15,17,18	2^{-23}
$(0,0,0,1,0,0,1,1,1,0,1,0,0,1,1,1) \xrightarrow{1r} (0,1,0,1,1,0,1,0,0,0,0,0,0,0,1,1)$	7,14,16	4,8,9,11,15	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,1,0,1,0,1,0,0,0) \xrightarrow{1r} (0,1,1,0,1,1,0,1,1,1,0,0,0,0,1,0)$	7	4,8,9,11,13	2^{-23}
$(0,0,0,1,0,0,1,1,1,0,1,0,1,0,0,1) \xrightarrow{1r} (1,0,0,1,0,0,1,0,0,0,1,1,1,1,0,0)$	7,16,17,18	4,8,9,11,13,17,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,1,0,1,0,1,0,1,0) \xrightarrow{1r} (1,0,1,0,1,1,0,0,1,1,0,0,0,0,1,0)$	7,18	4,8,9,11,13,15,18	2^{-23}
$(0,0,0,1,0,0,1,1,1,0,1,0,1,0,1,1) \xrightarrow{1r} (0,1,0,1,0,0,1,1,0,0,1,1,1,1,0,0)$	7,16,17	4,8,9,11,13,15,17	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,1,0,1,0,1,1,0,0) \xrightarrow{1r} (1,0,1,1,0,0,0,0,1,0,1,1,1,1,0,1)$	7,14,17,18	4,8,9,11,13,17,18	$2^{-28.5}$
$(0,0,0,1,0,0,1,1,1,0,1,0,1,1,0,1) \xrightarrow{1r} (0,1,0,0,1,1,1,1,0,1,0,0,0,0,1,1)$	7,14,16	4,8,9,11,13	2^{-23}
$(0,0,0,1,0,0,1,1,1,0,1,0,1,1,1,0) \xrightarrow{1r} (0,1,1,1,0,0,0,1,1,0,1,1,1,1,0,1)$	7,14,17	4,8,9,11,13,15,17	$2^{-28.5}$
$(0,0,0,1,0,0,1,1,1,0,1,0,1,1,1,1) \xrightarrow{1r} (1,0,0,0,1,1,1,0,0,1,0,0,0,0,1,1)$	7,14,16,18	4,8,9,11,13,15,18	2^{-23}
$(0,0,0,1,0,0,1,1,1,0,1,1,0,0,0,0) \xrightarrow{1r} (0,1,1,0,0,1,1,0,1,1,0,1,1,1,0,1)$	7,12,17	4,8,9,11,17	2^{-23}
$(0,0,0,1,0,0,1,1,1,0,1,1,0,0,0,1) \xrightarrow{1r} (1,0,0,1,1,0,0,1,0,0,1,0,0,0,1,1)$	7,12,16,18	4,8,9,11,18	$2^{-6.5}$
$(0,0,0,1,0,0,1,1,1,0,1,1,0,0,1,0) \xrightarrow{1r} (1,0,1,0,0,1,1,1,1,1,0,1,1,1,0,1)$	7,12,17,18	4,8,9,11,15,17,18	2^{-23}
$(0,0,0,1,0,0,1,1,1,0,1,1,0,0,1,1) \xrightarrow{1r} (0,1,0,1,1,0,0,0,0,0,1,0,0,0,1,1)$	7,12,16	4,8,9,11,15	$2^{-6.5}$
$(0,0,0,1,0,0,1,1,1,0,1,1,0,1,0,0) \xrightarrow{1r} (1,0,1,1,1,0,1,1,1,0,1,1,0,0,0,1,0)$	7,12,14,18	4,8,9,11,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,1,0,1,1,0,1,0,1) \xrightarrow{1r} (0,1,0,0,0,1,0,0,0,1,0,1,1,1,0,0)$	7,12,14,16,17	4,8,9,11,17	2^{-23}
$(0,0,0,1,0,0,1,1,1,0,1,1,0,1,1,0) \xrightarrow{1r} (0,1,1,1,1,0,1,0,1,0,1,0,0,0,1,0)$	7,12,14	4,8,9,11,15	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,1,0,1,1,0,1,1,1) \xrightarrow{1r} (1,0,0,0,0,1,0,1,0,1,0,1,1,1,0,0)$	7,12,14,16,17,18	4,8,9,11,15,17,18	2^{-23}
$(0,0,0,1,0,0,1,1,1,0,1,1,1,0,0,0) \xrightarrow{1r} (1,0,1,1,0,0,1,0,1,0,1,0,1,1,0,1)$	7,12,17,18	4,8,9,11,13,17,18	$2^{-28.5}$
$(0,0,0,1,0,0,1,1,1,0,1,1,1,0,0,1) \xrightarrow{1r} (0,1,0,0,1,1,0,1,0,1,1,0,0,0,1,1)$	7,12,16	4,8,9,11,13	2^{-12}
$(0,0,0,1,0,0,1,1,1,0,1,1,1,0,1,0) \xrightarrow{1r} (0,1,1,1,0,0,1,1,1,0,0,1,1,1,0,1)$	7,12,17	4,8,9,11,13,15,17	$2^{-28.5}$
$(0,0,0,1,0,0,1,1,1,0,1,1,1,0,1,1) \xrightarrow{1r} (1,0,0,0,1,1,0,0,0,1,1,0,0,0,1,1)$	7,12,16,18	4,8,9,11,13,15,18	2^{-12}
$(0,0,0,1,0,0,1,1,1,0,1,1,1,1,0,0) \xrightarrow{1r} (0,1,1,0,1,1,1,1,1,1,1,0,0,0,1,0)$	7,12,14	4,8,9,11,13	2^{-12}
$(0,0,0,1,0,0,1,1,1,0,1,1,1,1,0,1) \xrightarrow{1r} (1,0,0,1,0,0,0,0,0,0,0,0,1,1,1,0,0)$	7,12,14,16,17,18	4,8,9,11,13,17,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,1,0,1,1,1,1,1,0) \xrightarrow{1r} (1,0,1,0,1,1,1,0,1,1,1,0,0,0,1,0)$	7,12,14,18	4,8,9,11,13,15,18	2^{-12}
$(0,0,0,1,0,0,1,1,1,0,1,1,1,1,1,1) \xrightarrow{1r} (0,1,0,1,0,0,0,1,0,0,0,1,1,1,0,0)$	7,12,14,16,17	4,8,9,11,13,15,17	$2^{-17.5}$

Table 0.159 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	7,10,17,18	4,8,9,17,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	7,10,16	4,8,9	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	7,10,17	4,8,9,15,17	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	7,10,16,18	4,8,9,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	7,10,14	4,8,9	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	7,10,14,16,17,18	4,8,9,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	7,10,14,18	4,8,9,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	7,10,14,16,17	4,8,9,15,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	7,10,17	4,8,9,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	7,10,16,18	4,8,9,13,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	7,10,17,18	4,8,9,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	7,10,16	4,8,9,13,15	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	7,10,14,18	4,8,9,13,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	7,10,14,16,17	4,8,9,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	7,10,14	4,8,9,13,15	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	7,10,14,16,17,18	4,8,9,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	7,10,12	4,8,9	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	7,10,12,16,17,18	4,8,9,17,18	2^{-1}
$(0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	7,10,12,18	4,8,9,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	7,10,12,16,17	4,8,9,15,17	2^{-1}
$(0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	7,10,12,14,17,18	4,8,9,17,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	7,10,12,14,16	4,8,9	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	7,10,12,14,17	4,8,9,15,17	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	7,10,12,14,16,18	4,8,9,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	7,10,12,18	4,8,9,13,18	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	7,10,12,16,17	4,8,9,13,17	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	7,10,12	4,8,9,13,15	2^{-23}
$(0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	7,10,12,16,17,18	4,8,9,13,15,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	7,10,12,14,17	4,8,9,13,17	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	7,10,12,14,16,18	4,8,9,13,18	2^{-12}
$(0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	7,10,12,14,17,18	4,8,9,13,15,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	7,10,12,14,16	4,8,9,13,15	2^{-12}

Table 0.160 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,1,0,0,1,1,1,1,0,0,0,0,0) \xrightarrow{1r} (0,1,0,0,1,1,0,0,1,1,0,1,0,1,0,1)$	7,10,17	4,8,9,11,17	2^{-12}
$(0,0,0,1,0,0,1,1,1,1,0,0,0,0,1) \xrightarrow{1r} (1,0,1,1,0,0,1,1,0,0,1,0,1,0,1,1)$	7,10,16,18	4,8,9,11,18	$2^{-6.5}$
$(0,0,0,1,0,0,1,1,1,1,0,0,0,1,0) \xrightarrow{1r} (1,0,0,0,1,1,0,1,1,1,0,1,0,1,0,1)$	7,10,17,18	4,8,9,11,15,17,18	2^{-12}
$(0,0,0,1,0,0,1,1,1,1,0,0,0,1,1) \xrightarrow{1r} (0,1,1,1,0,0,1,0,0,0,1,0,1,0,1,1)$	7,10,16	4,8,9,11,15	$2^{-6.5}$
$(0,0,0,1,0,0,1,1,1,1,0,0,1,0,0) \xrightarrow{1r} (1,0,0,1,0,0,0,1,1,0,1,0,1,0,1,0)$	7,10,14,18	4,8,9,11,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,1,1,0,0,1,0,1) \xrightarrow{1r} (0,1,1,0,1,1,1,0,0,1,0,1,0,1,0,0)$	7,10,14,16,17	4,8,9,11,17	2^{-12}
$(0,0,0,1,0,0,1,1,1,1,0,0,1,1,0) \xrightarrow{1r} (0,1,0,1,0,0,0,0,1,0,1,0,1,0,1,0)$	7,10,14	4,8,9,11,15	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,1,1,0,0,1,1,1) \xrightarrow{1r} (1,0,1,0,1,1,1,1,0,1,0,1,0,1,0,0)$	7,10,14,16,17,18	4,8,9,11,15,17,18	2^{-12}
$(0,0,0,1,0,0,1,1,1,1,0,1,0,0,0) \xrightarrow{1r} (1,0,0,1,1,0,0,0,1,0,0,1,0,1,0,1)$	7,10,17,18	4,8,9,11,13,17,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,1,1,0,1,0,0,1) \xrightarrow{1r} (0,1,1,0,0,1,1,1,0,1,1,0,1,0,1,1)$	7,10,16	4,8,9,11,13	2^{-12}
$(0,0,0,1,0,0,1,1,1,1,0,1,0,1,0) \xrightarrow{1r} (0,1,0,1,1,0,0,1,1,0,0,1,0,1,0,1)$	7,10,17	4,8,9,11,13,15,17	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,1,1,0,1,0,1,1) \xrightarrow{1r} (1,0,1,0,0,1,1,0,0,1,1,0,1,0,1,1)$	7,10,16,18	4,8,9,11,13,15,18	2^{-12}
$(0,0,0,1,0,0,1,1,1,1,0,1,1,0,0) \xrightarrow{1r} (0,1,0,0,0,1,0,1,1,1,1,0,1,0,1,0)$	7,10,14	4,8,9,11,13	2^{-12}
$(0,0,0,1,0,0,1,1,1,1,0,1,1,0,1) \xrightarrow{1r} (1,0,1,1,1,0,1,0,0,0,0,1,0,1,0,0)$	7,10,14,16,17,18	4,8,9,11,13,17,18	$2^{-6.5}$
$(0,0,0,1,0,0,1,1,1,1,0,1,1,1,0) \xrightarrow{1r} (1,0,0,0,0,1,0,0,1,1,1,0,1,0,1,0)$	7,10,14,18	4,8,9,11,13,15,18	2^{-12}
$(0,0,0,1,0,0,1,1,1,1,0,1,1,1,1) \xrightarrow{1r} (0,1,1,1,1,0,1,1,0,0,0,1,0,1,0,0)$	7,10,14,16,17	4,8,9,11,13,15,17	$2^{-6.5}$
$(0,0,0,1,0,0,1,1,1,1,0,0,0,0,0) \xrightarrow{1r} (1,0,0,1,0,0,1,1,1,0,0,0,1,0,1,0)$	7,10,12,18	4,8,9,11,18	$2^{-28.5}$
$(0,0,0,1,0,0,1,1,1,1,0,0,0,1,0) \xrightarrow{1r} (0,1,1,0,1,1,0,0,0,1,1,1,0,1,0,0)$	7,10,12,16,17	4,8,9,11,17	2^{-12}
$(0,0,0,1,0,0,1,1,1,1,0,0,1,0,1) \xrightarrow{1r} (0,1,0,1,0,0,1,0,1,0,0,0,1,0,1,0)$	7,10,12	4,8,9,11,15	$2^{-28.5}$
$(0,0,0,1,0,0,1,1,1,1,0,0,1,1,1) \xrightarrow{1r} (1,0,1,0,1,1,0,1,0,1,1,1,0,1,0,0)$	7,10,12,16,17,18	4,8,9,11,15,17,18	2^{-12}
$(0,0,0,1,0,0,1,1,1,1,0,1,0,0,0) \xrightarrow{1r} (0,1,0,0,1,1,1,0,1,1,1,1,0,1,0,1)$	7,10,12,14,17	4,8,9,11,17	2^{-12}
$(0,0,0,1,0,0,1,1,1,1,0,1,0,1,0) \xrightarrow{1r} (1,0,1,1,0,0,0,1,0,0,0,0,1,0,1,1)$	7,10,12,14,16,18	4,8,9,11,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,1,1,0,1,1,1,0) \xrightarrow{1r} (1,0,0,0,1,1,1,1,1,1,1,1,0,1,0,1)$	7,10,12,14,17,18	4,8,9,11,15,17,18	2^{-12}
$(0,0,0,1,0,0,1,1,1,1,0,1,1,1,1) \xrightarrow{1r} (0,1,1,1,0,0,0,0,0,0,0,0,1,0,1,1)$	7,10,12,14,16	4,8,9,11,15	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,1,1,1,0,0,0,0) \xrightarrow{1r} (0,1,0,0,0,1,1,1,1,1,0,0,1,0,1,0)$	7,10,12	4,8,9,11,13	2^{-23}
$(0,0,0,1,0,0,1,1,1,1,1,0,0,1,0) \xrightarrow{1r} (1,0,1,1,1,0,0,0,0,0,1,1,0,1,0,0)$	7,10,12,16,17,18	4,8,9,11,13,17,18	$2^{-6.5}$
$(0,0,0,1,0,0,1,1,1,1,1,0,1,0,0) \xrightarrow{1r} (1,0,0,0,0,1,1,0,1,1,0,0,1,0,1,0)$	7,10,12,18	4,8,9,11,13,15,18	2^{-23}
$(0,0,0,1,0,0,1,1,1,1,1,0,1,1,1) \xrightarrow{1r} (0,1,1,1,1,0,0,1,0,0,1,1,0,1,0,0)$	7,10,12,16,17	4,8,9,11,13,15,17	$2^{-6.5}$
$(0,0,0,1,0,0,1,1,1,1,1,1,0,0,0) \xrightarrow{1r} (1,0,0,1,1,0,1,0,1,0,1,0,1,0,1,0)$	7,10,12,14,17,18	4,8,9,11,13,17,18	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,1,1,1,1,0,1,0) \xrightarrow{1r} (0,1,1,0,0,1,0,1,0,1,0,0,1,0,1,1)$	7,10,12,14,16	4,8,9,11,13	2^{-23}
$(0,0,0,1,0,0,1,1,1,1,1,1,1,0,0) \xrightarrow{1r} (0,1,0,1,1,0,1,1,1,0,1,1,0,1,0,1)$	7,10,12,14,17	4,8,9,11,13,15,17	$2^{-17.5}$
$(0,0,0,1,0,0,1,1,1,1,1,1,1,1,1) \xrightarrow{1r} (1,0,1,0,0,1,0,0,0,1,0,0,1,0,1,1)$	7,10,12,14,16,18	4,8,9,11,13,15,18	2^{-23}

Table 0.161 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	—	4,6	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	16,17,18	4,6,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	18	4,6,15,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	16,17	4,6,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	14,17,18	4,6,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	14,16	4,6	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	14,17	4,6,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	14,16,18	4,6,15,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	18	4,6,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	16,17	4,6,13,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	—	4,6,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	16,17,18	4,6,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	14,17	4,6,13,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	14,16,18	4,6,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	14,17,18	4,6,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	14,16	4,6,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	12,17,18	4,6,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	12,16	4,6	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	12,17	4,6,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	12,16,18	4,6,15,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	12,14	4,6	2^{-1}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	12,14,16,17,18	4,6,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	12,14,18	4,6,15,18	2^{-1}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	12,14,16,17	4,6,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	12,17	4,6,13,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	12,16,18	4,6,13,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	12,17,18	4,6,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	12,16	4,6,13,15	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	12,14,18	4,6,13,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	12,14,16,17	4,6,13,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	12,14	4,6,13,15	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	12,14,16,17,18	4,6,13,15,17,18	2^{-23}

Table 0.162 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	18	4,6,11,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	16,17	4,6,11,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	—	4,6,11,15	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	16,17,18	4,6,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	14,17	4,6,11,17	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	14,16,18	4,6,11,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	14,17,18	4,6,11,15,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	14,16	4,6,11,15	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	—	4,6,11,13	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	16,17,18	4,6,11,13,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	18	4,6,11,13,15,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	16,17	4,6,11,13,15,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	14,17,18	4,6,11,13,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	14,16	4,6,11,13	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	14,17	4,6,11,13,15,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	14,16,18	4,6,11,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	12,17	4,6,11,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	12,16,18	4,6,11,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	12,17,18	4,6,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	12,16	4,6,11,15	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	12,14,18	4,6,11,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	12,14,16,17	4,6,11,17	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	12,14	4,6,11,15	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	12,14,16,17,18	4,6,11,15,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	12,17,18	4,6,11,13,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	12,16	4,6,11,13	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	12,17	4,6,11,13,15,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	12,16,18	4,6,11,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	12,14	4,6,11,13	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	12,14,16,17,18	4,6,11,13,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	12,14,18	4,6,11,13,15,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	12,14,16,17	4,6,11,13,15,17	2^{-23}

Table 0.163 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	10,17,18	4,6,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	10,16	4,6	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	10,17	4,6,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	10,16,18	4,6,15,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	10,14	4,6	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	10,14,16,17,18	4,6,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	10,14,18	4,6,15,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	10,14,16,17	4,6,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	10,17	4,6,13,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	10,16,18	4,6,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	10,17,18	4,6,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	10,16	4,6,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	10,14,18	4,6,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	10,14,16,17	4,6,13,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	10,14	4,6,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	10,14,16,17,18	4,6,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	10,12	4,6	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	10,12,16,17,18	4,6,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	10,12,18	4,6,15,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	10,12,16,17	4,6,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	10,12,14,17,18	4,6,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	10,12,14,16	4,6	2^{-34}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	10,12,14,17	4,6,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	10,12,14,16,18	4,6,15,18	2^{-34}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	10,12,18	4,6,13,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	10,12,16,17	4,6,13,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	10,12	4,6,13,15	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	10,12,16,17,18	4,6,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	10,12,14,17	4,6,13,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	10,12,14,16,18	4,6,13,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	10,12,14,17,18	4,6,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	10,12,14,16	4,6,13,15	$2^{-28.5}$

Table 0.164 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	10,17	4,6,11,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	10,16,18	4,6,11,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	10,17,18	4,6,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	10,16	4,6,11,15	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	10,14,18	4,6,11,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	10,14,16,17	4,6,11,17	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	10,14	4,6,11,15	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	10,14,16,17,18	4,6,11,15,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	10,17,18	4,6,11,13,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	10,16	4,6,11,13	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	10,17	4,6,11,13,15,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	10,16,18	4,6,11,13,15,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	10,14	4,6,11,13	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	10,14,16,17,18	4,6,11,13,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	10,14,18	4,6,11,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	10,14,16,17	4,6,11,13,15,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	10,12,18	4,6,11,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	10,12,16,17	4,6,11,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	10,12	4,6,11,15	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	10,12,16,17,18	4,6,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	10,12,14,17	4,6,11,17	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	10,12,14,16,18	4,6,11,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	10,12,14,17,18	4,6,11,15,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	10,12,14,16	4,6,11,15	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	10,12	4,6,11,13	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	10,12,16,17,18	4,6,11,13,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	10,12,18	4,6,11,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	10,12,16,17	4,6,11,13,15,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	10,12,14,17,18	4,6,11,13,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	10,12,14,16	4,6,11,13	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	10,12,14,17	4,6,11,13,15,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	10,12,14,16,18	4,6,11,13,15,18	$2^{-28.5}$

Table 0.165 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	18	4,6,9,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	16,17	4,6,9,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	—	4,6,9,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	16,17,18	4,6,9,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	14,17	4,6,9,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	14,16,18	4,6,9,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	14,17,18	4,6,9,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	14,16	4,6,9,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	—	4,6,9,13	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	16,17,18	4,6,9,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	18	4,6,9,13,15,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	16,17	4,6,9,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	14,17,18	4,6,9,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	14,16	4,6,9,13	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	14,17	4,6,9,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	14,16,18	4,6,9,13,15,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	12,17	4,6,9,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	12,16,18	4,6,9,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	12,17,18	4,6,9,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	12,16	4,6,9,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	12,14,18	4,6,9,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	12,14,16,17	4,6,9,17	2^{-34}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	12,14	4,6,9,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	12,14,16,17,18	4,6,9,15,17,18	2^{-34}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	12,17,18	4,6,9,13,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	12,16	4,6,9,13	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	12,17	4,6,9,13,15,17	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	12,16,18	4,6,9,13,15,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	12,14	4,6,9,13	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	12,14,16,17,18	4,6,9,13,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	12,14,18	4,6,9,13,15,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	12,14,16,17	4,6,9,13,15,17	$2^{-28.5}$

Table 0.166 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	—	4,6,9,11	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	16,17,18	4,6,9,11,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	18	4,6,9,11,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	16,17	4,6,9,11,15,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	14,17,18	4,6,9,11,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	14,16	4,6,9,11	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	14,17	4,6,9,11,15,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	14,16,18	4,6,9,11,15,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	18	4,6,9,11,13,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	16,17	4,6,9,11,13,17	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	—	4,6,9,11,13,15	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	16,17,18	4,6,9,11,13,15,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	14,17	4,6,9,11,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	14,16,18	4,6,9,11,13,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	14,17,18	4,6,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	14,16	4,6,9,11,13,15	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	12,17,18	4,6,9,11,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	12,16	4,6,9,11	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	12,17	4,6,9,11,15,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	12,16,18	4,6,9,11,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	12,14	4,6,9,11	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	12,14,16,17,18	4,6,9,11,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	12,14,18	4,6,9,11,15,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	12,14,16,17	4,6,9,11,15,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	12,17	4,6,9,11,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	12,16,18	4,6,9,11,13,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	12,17,18	4,6,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	12,16	4,6,9,11,13,15	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	12,14,18	4,6,9,11,13,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	12,14,16,17	4,6,9,11,13,17	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	12,14	4,6,9,11,13,15	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	12,14,16,17,18	4,6,9,11,13,15,17,18	$2^{-28.5}$

Table 0.167 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	10,17	4,6,9,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	10,16,18	4,6,9,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	10,17,18	4,6,9,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	10,16	4,6,9,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	10,14,18	4,6,9,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	10,14,16,17	4,6,9,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	10,14	4,6,9,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	10,14,16,17,18	4,6,9,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	10,17,18	4,6,9,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	10,16	4,6,9,13	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	10,17	4,6,9,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	10,16,18	4,6,9,13,15,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	10,14	4,6,9,13	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	10,14,16,17,18	4,6,9,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	10,14,18	4,6,9,13,15,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	10,14,16,17	4,6,9,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	10,12,18	4,6,9,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	10,12,16,17	4,6,9,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	10,12	4,6,9,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	10,12,16,17,18	4,6,9,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	10,12,14,17	4,6,9,17	2^{-1}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	10,12,14,16,18	4,6,9,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	10,12,14,17,18	4,6,9,15,17,18	2^{-1}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	10,12,14,16	4,6,9,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	10,12	4,6,9,13	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	10,12,16,17,18	4,6,9,13,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	10,12,18	4,6,9,13,15,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	10,12,16,17	4,6,9,13,15,17	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	10,12,14,17,18	4,6,9,13,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	10,12,14,16	4,6,9,13	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	10,12,14,17	4,6,9,13,15,17	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	10,12,14,16,18	4,6,9,13,15,18	2^{-23}

Table 0.168 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	10,17,18	4,6,9,11,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	10,16	4,6,9,11	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	10,17	4,6,9,11,15,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	10,16,18	4,6,9,11,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	10,14	4,6,9,11	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	10,14,16,17,18	4,6,9,11,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	10,14,18	4,6,9,11,15,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	10,14,16,17	4,6,9,11,15,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	10,17	4,6,9,11,13,17	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	10,16,18	4,6,9,11,13,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	10,17,18	4,6,9,11,13,15,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	10,16	4,6,9,11,13,15	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	10,14,18	4,6,9,11,13,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	10,14,16,17	4,6,9,11,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	10,14	4,6,9,11,13,15	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	10,14,16,17,18	4,6,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	10,12	4,6,9,11	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	10,12,16,17,18	4,6,9,11,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	10,12,18	4,6,9,11,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	10,12,16,17	4,6,9,11,15,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	10,12,14,17,18	4,6,9,11,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	10,12,14,16	4,6,9,11	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	10,12,14,17	4,6,9,11,15,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	10,12,14,16,18	4,6,9,11,15,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	10,12,18	4,6,9,11,13,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	10,12,16,17	4,6,9,11,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	10,12	4,6,9,11,13,15	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	10,12,16,17,18	4,6,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	10,12,14,17	4,6,9,11,13,17	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	10,12,14,16,18	4,6,9,11,13,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	10,12,14,17,18	4,6,9,11,13,15,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	10,12,14,16	4,6,9,11,13,15	2^{-23}

Table 0.169 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	17,18	4,6,8,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	16	4,6,8	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	17	4,6,8,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	16,18	4,6,8,15,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	14	4,6,8	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	14,16,17,18	4,6,8,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	14,18	4,6,8,15,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	14,16,17	4,6,8,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	17	4,6,8,13,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	16,18	4,6,8,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	17,18	4,6,8,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	16	4,6,8,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	14,18	4,6,8,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	14,16,17	4,6,8,13,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	14	4,6,8,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	14,16,17,18	4,6,8,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	12	4,6,8	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	12,16,17,18	4,6,8,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	12,18	4,6,8,15,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	12,16,17	4,6,8,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	12,14,17,18	4,6,8,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	12,14,16	4,6,8	2^{-1}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	12,14,17	4,6,8,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	12,14,16,18	4,6,8,15,18	2^{-1}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	12,18	4,6,8,13,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	12,16,17	4,6,8,13,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	12	4,6,8,13,15	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	12,16,17,18	4,6,8,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	12,14,17	4,6,8,13,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	12,14,16,18	4,6,8,13,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	12,14,17,18	4,6,8,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	12,14,16	4,6,8,13,15	$2^{-6.5}$

Table 0.170 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,1,0,1,0,1,0,0,1,0,0,0,0,0) \xrightarrow{1r} (0,0,1,1,0,0,1,1,1,0,1,0,0,1,0,1)$	17	4,6,8,11,17	$2^{-17.5}$
$(0,0,0,1,0,1,0,1,0,0,1,0,0,0,0,1) \xrightarrow{1r} (1,1,0,0,1,1,0,0,0,1,0,1,1,0,1,1)$	16,18	4,6,8,11,18	2^{-12}
$(0,0,0,1,0,1,0,1,0,0,1,0,0,0,1,0) \xrightarrow{1r} (1,1,1,1,0,0,1,0,1,0,1,0,0,1,0,1)$	17,18	4,6,8,11,15,17,18	$2^{-17.5}$
$(0,0,0,1,0,1,0,1,0,0,1,0,0,0,1,1) \xrightarrow{1r} (0,0,0,0,1,1,0,1,0,1,0,1,1,0,1,1)$	16	4,6,8,11,15	2^{-12}
$(0,0,0,1,0,1,0,1,0,0,1,0,0,1,0,0) \xrightarrow{1r} (1,1,1,0,1,1,1,0,1,1,0,1,1,0,1,0)$	14,18	4,6,8,11,18	2^{-12}
$(0,0,0,1,0,1,0,1,0,0,1,0,0,1,0,1) \xrightarrow{1r} (0,0,0,1,0,0,0,1,0,0,1,0,0,1,0,0)$	14,16,17	4,6,8,11,17	$2^{-6.5}$
$(0,0,0,1,0,1,0,1,0,0,1,0,0,1,1,0) \xrightarrow{1r} (0,0,1,0,1,1,1,1,1,1,0,1,1,0,1,0)$	14	4,6,8,11,15	2^{-12}
$(0,0,0,1,0,1,0,1,0,0,1,0,0,1,1,1) \xrightarrow{1r} (1,1,0,1,0,0,0,0,0,0,1,0,0,1,0,0)$	14,16,17,18	4,6,8,11,15,17,18	$2^{-6.5}$
$(0,0,0,1,0,1,0,1,0,0,1,0,1,0,0,0) \xrightarrow{1r} (1,1,1,0,0,1,1,1,1,1,1,0,0,1,0,1)$	17,18	4,6,8,11,13,17,18	2^{-12}
$(0,0,0,1,0,1,0,1,0,0,1,0,1,0,0,1) \xrightarrow{1r} (0,0,0,1,1,0,0,0,0,0,0,1,1,0,1,1)$	16	4,6,8,11,13	$2^{-6.5}$
$(0,0,0,1,0,1,0,1,0,0,1,0,1,0,1,0) \xrightarrow{1r} (0,0,1,0,0,1,1,0,1,1,1,0,0,1,0,1)$	17	4,6,8,11,13,15,17	2^{-12}
$(0,0,0,1,0,1,0,1,0,0,1,0,1,0,1,1) \xrightarrow{1r} (1,1,0,1,1,0,0,1,0,0,0,1,1,0,1,1)$	16,18	4,6,8,11,13,15,18	$2^{-6.5}$
$(0,0,0,1,0,1,0,1,0,0,1,0,1,1,0,0) \xrightarrow{1r} (0,0,1,1,1,0,1,0,1,0,0,1,1,0,1,0)$	14	4,6,8,11,13	$2^{-17.5}$
$(0,0,0,1,0,1,0,1,0,0,1,0,1,1,0,1) \xrightarrow{1r} (1,1,0,0,0,1,0,1,0,1,1,0,0,1,0,0)$	14,16,17,18	4,6,8,11,13,17,18	2^{-12}
$(0,0,0,1,0,1,0,1,0,0,1,0,1,1,1,0) \xrightarrow{1r} (1,1,1,1,1,0,1,1,1,0,0,1,1,0,1,0)$	14,18	4,6,8,11,13,15,18	$2^{-17.5}$
$(0,0,0,1,0,1,0,1,0,0,1,0,1,1,1,1) \xrightarrow{1r} (0,0,0,0,0,1,0,0,0,1,1,0,0,1,0,0)$	14,16,17	4,6,8,11,13,15,17	2^{-12}
$(0,0,0,1,0,1,0,1,0,0,1,1,0,0,0,0) \xrightarrow{1r} (1,1,1,0,1,1,0,0,1,1,1,1,1,0,1,0)$	12,18	4,6,8,11,18	2^{-12}
$(0,0,0,1,0,1,0,1,0,0,1,1,0,0,0,1) \xrightarrow{1r} (0,0,0,1,0,0,1,1,0,0,0,0,0,1,0,0)$	12,16,17	4,6,8,11,17	$2^{-17.5}$
$(0,0,0,1,0,1,0,1,0,0,1,1,0,0,1,0) \xrightarrow{1r} (0,0,1,0,1,1,0,1,1,1,1,1,1,1,0,1,0)$	12	4,6,8,11,15	2^{-12}
$(0,0,0,1,0,1,0,1,0,0,1,1,0,0,1,1) \xrightarrow{1r} (1,1,0,1,0,0,1,0,0,0,0,0,0,0,1,0,0)$	12,16,17,18	4,6,8,11,15,17,18	$2^{-17.5}$
$(0,0,0,1,0,1,0,1,0,0,1,1,0,1,0,0) \xrightarrow{1r} (0,0,1,1,0,0,0,1,1,0,0,0,0,1,0,1)$	12,14,17	4,6,8,11,17	$2^{-28.5}$
$(0,0,0,1,0,1,0,1,0,0,1,1,0,1,0,1) \xrightarrow{1r} (1,1,0,0,1,1,1,0,0,1,1,1,1,0,1,1)$	12,14,16,18	4,6,8,11,18	2^{-12}
$(0,0,0,1,0,1,0,1,0,0,1,1,0,1,1,0) \xrightarrow{1r} (1,1,1,1,0,0,0,0,1,0,0,0,0,1,0,1)$	12,14,17,18	4,6,8,11,15,17,18	$2^{-28.5}$
$(0,0,0,1,0,1,0,1,0,0,1,1,0,1,1,1) \xrightarrow{1r} (0,0,0,0,1,1,1,1,0,1,1,1,1,0,1,1)$	12,14,16	4,6,8,11,15	2^{-12}
$(0,0,0,1,0,1,0,1,0,0,1,1,1,0,0,0) \xrightarrow{1r} (0,0,1,1,1,0,0,0,1,0,1,1,1,1,0,1,0)$	12	4,6,8,11,13	$2^{-17.5}$
$(0,0,0,1,0,1,0,1,0,0,1,1,1,0,0,1) \xrightarrow{1r} (1,1,0,0,0,1,1,1,0,1,0,0,0,1,0,0)$	12,16,17,18	4,6,8,11,13,17,18	2^{-23}
$(0,0,0,1,0,1,0,1,0,0,1,1,1,0,1,0) \xrightarrow{1r} (1,1,1,1,1,0,0,1,1,0,1,1,1,1,0,1,0)$	12,18	4,6,8,11,13,15,18	$2^{-17.5}$
$(0,0,0,1,0,1,0,1,0,0,1,1,1,0,1,1) \xrightarrow{1r} (0,0,0,0,0,1,1,0,0,1,0,0,0,1,0,0)$	12,16,17	4,6,8,11,13,15,17	2^{-23}
$(0,0,0,1,0,1,0,1,0,0,1,1,1,1,0,0) \xrightarrow{1r} (1,1,1,0,0,1,0,1,1,1,0,0,0,1,0,1)$	12,14,17,18	4,6,8,11,13,17,18	2^{-23}
$(0,0,0,1,0,1,0,1,0,0,1,1,1,1,0,1) \xrightarrow{1r} (0,0,0,1,1,0,1,0,0,0,1,1,1,0,1,1)$	12,14,16	4,6,8,11,13	$2^{-6.5}$
$(0,0,0,1,0,1,0,1,0,0,1,1,1,1,1,0) \xrightarrow{1r} (0,0,1,0,0,1,0,0,1,1,0,0,0,1,0,1)$	12,14,17	4,6,8,11,13,15,17	2^{-23}
$(0,0,0,1,0,1,0,1,0,0,1,1,1,1,1,1) \xrightarrow{1r} (1,1,0,1,1,0,1,1,0,0,1,1,1,0,1,1)$	12,14,16,18	4,6,8,11,13,15,18	$2^{-6.5}$

Table 0.171 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	10	4,6,8	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	10,16,17,18	4,6,8,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	10,18	4,6,8,15,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	10,16,17	4,6,8,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	10,14,17,18	4,6,8,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	10,14,16	4,6,8	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	10,14,17	4,6,8,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	10,14,16,18	4,6,8,15,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	10,18	4,6,8,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	10,16,17	4,6,8,13,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	10	4,6,8,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	10,16,17,18	4,6,8,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	10,14,17	4,6,8,13,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	10,14,16,18	4,6,8,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	10,14,17,18	4,6,8,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	10,14,16	4,6,8,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	10,12,17,18	4,6,8,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	10,12,16	4,6,8	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	10,12,17	4,6,8,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	10,12,16,18	4,6,8,15,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	10,12,14	4,6,8	2^{-34}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	10,12,14,16,17,18	4,6,8,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	10,12,14,18	4,6,8,15,18	2^{-34}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	10,12,14,16,17	4,6,8,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	10,12,17	4,6,8,13,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	10,12,16,18	4,6,8,13,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	10,12,17,18	4,6,8,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	10,12,16	4,6,8,13,15	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	10,12,14,18	4,6,8,13,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	10,12,14,16,17	4,6,8,13,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	10,12,14	4,6,8,13,15	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	10,12,14,16,17,18	4,6,8,13,15,17,18	2^{-12}

Table 0.172 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	10,18	4,6,8,11,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	10,16,17	4,6,8,11,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	10	4,6,8,11,15	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	10,16,17,18	4,6,8,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	10,14,17	4,6,8,11,17	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	10,14,16,18	4,6,8,11,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	10,14,17,18	4,6,8,11,15,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	10,14,16	4,6,8,11,15	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	10	4,6,8,11,13	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	10,16,17,18	4,6,8,11,13,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	10,18	4,6,8,11,13,15,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	10,16,17	4,6,8,11,13,15,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	10,14,17,18	4,6,8,11,13,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	10,14,16	4,6,8,11,13	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	10,14,17	4,6,8,11,13,15,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	10,14,16,18	4,6,8,11,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	10,12,17	4,6,8,11,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	10,12,16,18	4,6,8,11,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	10,12,17,18	4,6,8,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	10,12,16	4,6,8,11,15	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	10,12,14,18	4,6,8,11,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	10,12,14,16,17	4,6,8,11,17	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	10,12,14	4,6,8,11,15	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	10,12,14,16,17,18	4,6,8,11,15,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	10,12,17,18	4,6,8,11,13,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	10,12,16	4,6,8,11,13	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	10,12,17	4,6,8,11,13,15,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	10,12,16,18	4,6,8,11,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	10,12,14	4,6,8,11,13	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	10,12,14,16,17,18	4,6,8,11,13,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	10,12,14,18	4,6,8,11,13,15,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	10,12,14,16,17	4,6,8,11,13,15,17	2^{-12}

Table 0.173 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	17	4,6,8,9,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	16,18	4,6,8,9,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	17,18	4,6,8,9,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	16	4,6,8,9,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	14,18	4,6,8,9,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	14,16,17	4,6,8,9,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	14	4,6,8,9,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	14,16,17,18	4,6,8,9,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	17,18	4,6,8,9,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	16	4,6,8,9,13	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	17	4,6,8,9,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	16,18	4,6,8,9,13,15,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	14	4,6,8,9,13	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	14,16,17,18	4,6,8,9,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	14,18	4,6,8,9,13,15,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	14,16,17	4,6,8,9,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	12,18	4,6,8,9,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	12,16,17	4,6,8,9,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	12	4,6,8,9,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	12,16,17,18	4,6,8,9,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	12,14,17	4,6,8,9,17	2^{-34}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	12,14,16,18	4,6,8,9,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	12,14,17,18	4,6,8,9,15,17,18	2^{-34}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	12,14,16	4,6,8,9,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	12	4,6,8,9,13	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	12,16,17,18	4,6,8,9,13,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	12,18	4,6,8,9,13,15,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	12,16,17	4,6,8,9,13,15,17	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	12,14,17,18	4,6,8,9,13,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	12,14,16	4,6,8,9,13	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	12,14,17	4,6,8,9,13,15,17	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	12,14,16,18	4,6,8,9,13,15,18	2^{-12}

Table 0.174 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,1,0,1,0,1,1,0,1,0,0,0,0,0) \xrightarrow{1r} (1,0,1,0,0,1,1,0,1,1,1,1,0,0,0,1)$	17,18	4,6,8,9,11,17,18	2^{-23}
$(0,0,0,1,0,1,0,1,1,0,1,0,0,0,0,1) \xrightarrow{1r} (0,1,0,1,1,0,0,1,0,0,0,0,1,1,1,1)$	16	4,6,8,9,11	$2^{-17.5}$
$(0,0,0,1,0,1,0,1,1,0,1,0,0,0,1,0) \xrightarrow{1r} (0,1,1,0,0,1,1,1,1,1,1,1,0,0,0,1)$	17	4,6,8,9,11,15,17	2^{-23}
$(0,0,0,1,0,1,0,1,1,0,1,0,0,0,1,1) \xrightarrow{1r} (1,0,0,1,1,0,0,0,0,0,0,0,1,1,1,1)$	16,18	4,6,8,9,11,15,18	$2^{-17.5}$
$(0,0,0,1,0,1,0,1,1,0,1,0,0,1,0,0) \xrightarrow{1r} (0,1,1,1,0,1,1,1,0,0,0,1,1,1,0,0)$	14	4,6,8,9,11	$2^{-28.5}$
$(0,0,0,1,0,1,0,1,1,0,1,0,0,1,0,1) \xrightarrow{1r} (1,0,0,0,0,1,0,0,0,1,1,1,0,0,0,0)$	14,16,17,18	4,6,8,9,11,17,18	2^{-23}
$(0,0,0,1,0,1,0,1,1,0,1,0,0,1,1,0) \xrightarrow{1r} (1,0,1,1,1,0,1,0,1,0,0,0,1,1,1,0)$	14,18	4,6,8,9,11,15,18	$2^{-28.5}$
$(0,0,0,1,0,1,0,1,1,0,1,0,0,1,1,1) \xrightarrow{1r} (0,1,0,0,0,1,0,1,0,1,1,1,0,0,0,0)$	14,16,17	4,6,8,9,11,15,17	2^{-23}
$(0,0,0,1,0,1,0,1,1,0,1,0,1,0,0,0) \xrightarrow{1r} (0,1,1,1,0,0,1,0,1,0,1,1,0,0,0,1)$	17	4,6,8,9,11,13,17	$2^{-28.5}$
$(0,0,0,1,0,1,0,1,1,0,1,0,1,0,0,1) \xrightarrow{1r} (1,0,0,0,1,1,0,1,0,1,0,0,1,1,1,1)$	16,18	4,6,8,9,11,13,18	2^{-23}
$(0,0,0,1,0,1,0,1,1,0,1,0,1,0,1,0) \xrightarrow{1r} (1,0,1,1,0,0,1,1,1,0,1,1,0,0,0,1)$	17,18	4,6,8,9,11,13,15,17,18	$2^{-28.5}$
$(0,0,0,1,0,1,0,1,1,0,1,0,1,0,1,1) \xrightarrow{1r} (0,1,0,0,1,1,0,0,0,1,0,0,1,1,1,1)$	16	4,6,8,9,11,13,15	2^{-23}
$(0,0,0,1,0,1,0,1,1,0,1,0,1,1,0,0) \xrightarrow{1r} (1,0,1,0,1,1,1,1,1,1,0,0,1,1,1,0)$	14,18	4,6,8,9,11,13,18	2^{-23}
$(0,0,0,1,0,1,0,1,1,0,1,0,1,1,0,1) \xrightarrow{1r} (0,1,0,1,0,0,0,0,0,0,0,1,1,0,0,0)$	14,16,17	4,6,8,9,11,13,17	$2^{-17.5}$
$(0,0,0,1,0,1,0,1,1,0,1,0,1,1,1,0) \xrightarrow{1r} (0,1,1,0,1,1,1,0,1,1,0,0,1,1,1,0)$	14	4,6,8,9,11,13,15	2^{-23}
$(0,0,0,1,0,1,0,1,1,0,1,0,1,1,1,1) \xrightarrow{1r} (1,0,0,1,0,0,0,1,0,0,1,1,0,0,0,0)$	14,16,17,18	4,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(0,0,0,1,0,1,0,1,1,0,1,0,0,0,0,0) \xrightarrow{1r} (0,1,1,1,0,0,1,1,0,1,0,1,1,1,0,0)$	12	4,6,8,9,11	$2^{-17.5}$
$(0,0,0,1,0,1,0,1,1,0,1,0,0,0,0,1) \xrightarrow{1r} (1,0,0,0,0,1,1,0,0,1,0,1,0,0,0,0)$	12,16,17,18	4,6,8,9,11,17,18	2^{-23}
$(0,0,0,1,0,1,0,1,1,0,1,0,0,0,1,0) \xrightarrow{1r} (1,0,1,1,1,0,0,0,1,0,1,0,1,1,1,0)$	12,18	4,6,8,9,11,15,18	$2^{-17.5}$
$(0,0,0,1,0,1,0,1,1,0,1,0,0,0,1,1) \xrightarrow{1r} (0,1,0,0,0,1,1,1,0,1,0,1,0,0,0,0)$	12,16,17	4,6,8,9,11,15,17	2^{-23}
$(0,0,0,1,0,1,0,1,1,0,1,0,1,0,0,0) \xrightarrow{1r} (1,0,1,0,0,1,0,0,1,1,0,1,0,0,0,1)$	12,14,17,18	4,6,8,9,11,17,18	2^{-23}
$(0,0,0,1,0,1,0,1,1,0,1,0,1,0,1,0) \xrightarrow{1r} (0,1,0,1,1,0,1,1,0,0,1,0,1,1,1,1)$	12,14,16	4,6,8,9,11	$2^{-6.5}$
$(0,0,0,1,0,1,0,1,1,0,1,0,1,1,0,1) \xrightarrow{1r} (0,1,1,0,0,1,0,1,1,1,0,1,0,0,0,1)$	12,14,17	4,6,8,9,11,15,17	2^{-23}
$(0,0,0,1,0,1,0,1,1,0,1,0,1,1,1,1) \xrightarrow{1r} (1,0,0,1,1,0,1,0,0,0,1,0,1,1,1,1)$	12,14,16,18	4,6,8,9,11,15,18	$2^{-6.5}$
$(0,0,0,1,0,1,0,1,1,0,1,0,1,1,0,0) \xrightarrow{1r} (1,0,1,0,1,1,0,1,1,1,1,0,1,1,1,0)$	12,18	4,6,8,9,11,13,18	2^{-12}
$(0,0,0,1,0,1,0,1,1,0,1,0,1,1,0,0) \xrightarrow{1r} (0,1,0,1,0,0,1,0,0,0,0,1,0,0,0,0)$	12,16,17	4,6,8,9,11,13,17	$2^{-17.5}$
$(0,0,0,1,0,1,0,1,1,0,1,0,1,1,0,1) \xrightarrow{1r} (0,1,1,0,1,1,0,0,1,1,1,0,1,1,1,0)$	12	4,6,8,9,11,13,15	2^{-12}
$(0,0,0,1,0,1,0,1,1,0,1,0,1,1,0,1) \xrightarrow{1r} (1,0,0,1,0,0,1,1,0,0,0,1,0,0,0,0)$	12,16,17,18	4,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(0,0,0,1,0,1,0,1,1,0,1,0,1,1,1,0) \xrightarrow{1r} (0,1,1,1,0,0,0,0,1,0,0,1,0,0,0,1)$	12,14,17	4,6,8,9,11,13,17	$2^{-28.5}$
$(0,0,0,1,0,1,0,1,1,0,1,0,1,1,1,0) \xrightarrow{1r} (1,0,0,0,1,1,1,1,0,1,1,0,1,1,1,1)$	12,14,16,18	4,6,8,9,11,13,18	2^{-12}
$(0,0,0,1,0,1,0,1,1,0,1,0,1,1,1,1) \xrightarrow{1r} (1,0,1,1,0,0,0,1,1,0,0,1,0,0,0,1)$	12,14,17,18	4,6,8,9,11,13,15,17,18	$2^{-28.5}$
$(0,0,0,1,0,1,0,1,1,0,1,0,1,1,1,1) \xrightarrow{1r} (0,1,0,0,1,1,1,0,0,1,1,0,1,1,1,1)$	12,14,16	4,6,8,9,11,13,15	2^{-12}

Table 0.175 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	10,18	4,6,8,9,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	10,16,17	4,6,8,9,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	10	4,6,8,9,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	10,16,17,18	4,6,8,9,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	10,14,17	4,6,8,9,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	10,14,16,18	4,6,8,9,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	10,14,17,18	4,6,8,9,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	10,14,16	4,6,8,9,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	10	4,6,8,9,13	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	10,16,17,18	4,6,8,9,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	10,18	4,6,8,9,13,15,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	10,16,17	4,6,8,9,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	10,14,17,18	4,6,8,9,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	10,14,16	4,6,8,9,13	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	10,14,17	4,6,8,9,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	10,14,16,18	4,6,8,9,13,15,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	10,12,17	4,6,8,9,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	10,12,16,18	4,6,8,9,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	10,12,17,18	4,6,8,9,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	10,12,16	4,6,8,9,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	10,12,14,18	4,6,8,9,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	10,12,14,16,17	4,6,8,9,17	2^{-1}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	10,12,14	4,6,8,9,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	10,12,14,16,17,18	4,6,8,9,15,17,18	2^{-1}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	10,12,17,18	4,6,8,9,13,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	10,12,16	4,6,8,9,13	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	10,12,17	4,6,8,9,13,15,17	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	10,12,16,18	4,6,8,9,13,15,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	10,12,14	4,6,8,9,13	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	10,12,14,16,17,18	4,6,8,9,13,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	10,12,14,18	4,6,8,9,13,15,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	10,12,14,16,17	4,6,8,9,13,15,17	$2^{-6.5}$

Table 0.176 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	10	4,6,8,9,11	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	10,16,17,18	4,6,8,9,11,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	10,18	4,6,8,9,11,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	10,16,17	4,6,8,9,11,15,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	10,14,17,18	4,6,8,9,11,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	10,14,16	4,6,8,9,11	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	10,14,17	4,6,8,9,11,15,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	10,14,16,18	4,6,8,9,11,15,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	10,18	4,6,8,9,11,13,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	10,16,17	4,6,8,9,11,13,17	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	10	4,6,8,9,11,13,15	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	10,16,17,18	4,6,8,9,11,13,15,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	10,14,17	4,6,8,9,11,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	10,14,16,18	4,6,8,9,11,13,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	10,14,17,18	4,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	10,14,16	4,6,8,9,11,13,15	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	10,12,17,18	4,6,8,9,11,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	10,12,16	4,6,8,9,11	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	10,12,17	4,6,8,9,11,15,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	10,12,16,18	4,6,8,9,11,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	10,12,14	4,6,8,9,11	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	10,12,14,16,17,18	4,6,8,9,11,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	10,12,14,18	4,6,8,9,11,15,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	10,12,14,16,17	4,6,8,9,11,15,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	10,12,17	4,6,8,9,11,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	10,12,16,18	4,6,8,9,11,13,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	10,12,17,18	4,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	10,12,16	4,6,8,9,11,13,15	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	10,12,14,18	4,6,8,9,11,13,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	10,12,14,16,17	4,6,8,9,11,13,17	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	10,12,14	4,6,8,9,11,13,15	2^{-23}
$(0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	10,12,14,16,17,18	4,6,8,9,11,13,15,17,18	$2^{-6.5}$

Table 0.177 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,1,0,1,1,0,0,0,0,0,0,0,0,0) \xrightarrow{1r} (1,1,0,0,1,0,0,0,0,0,0,0,1,1,0,0)$	7,18	4,6,18	2^{-12}
$(0,0,0,1,0,1,1,0,0,0,0,0,0,0,0,1) \xrightarrow{1r} (0,0,1,1,0,1,1,1,1,1,1,1,0,0,1,0)$	7,16,17	4,6,17	$2^{-17.5}$
$(0,0,0,1,0,1,1,0,0,0,0,0,0,0,1,0) \xrightarrow{1r} (0,0,0,0,1,0,0,1,0,0,0,0,1,1,0,0)$	7	4,6,15	2^{-12}
$(0,0,0,1,0,1,1,0,0,0,0,0,0,0,1,1) \xrightarrow{1r} (1,1,1,1,0,1,1,0,1,1,1,1,0,0,1,0)$	7,16,17,18	4,6,15,17,18	$2^{-17.5}$
$(0,0,0,1,0,1,1,0,0,0,0,0,0,1,0,0) \xrightarrow{1r} (0,0,0,1,0,1,0,1,0,1,1,1,0,0,1,1)$	7,14,17	4,6,17	$2^{-17.5}$
$(0,0,0,1,0,1,1,0,0,0,0,0,0,1,0,1) \xrightarrow{1r} (1,1,1,0,1,0,1,0,1,0,0,0,1,1,0,1)$	7,14,16,18	4,6,18	2^{-23}
$(0,0,0,1,0,1,1,0,0,0,0,0,0,1,1,0) \xrightarrow{1r} (1,1,0,1,0,1,0,0,0,1,1,1,0,0,1,1)$	7,14,17,18	4,6,15,17,18	$2^{-17.5}$
$(0,0,0,1,0,1,1,0,0,0,0,0,0,1,1,1) \xrightarrow{1r} (0,0,1,0,1,0,1,1,1,0,0,0,1,1,0,1)$	7,14,16	4,6,15	2^{-23}
$(0,0,0,1,0,1,1,0,0,0,0,0,1,0,0,0) \xrightarrow{1r} (0,0,0,1,1,1,0,0,0,1,0,0,1,1,0,0)$	7	4,6,13	$2^{-17.5}$
$(0,0,0,1,0,1,1,0,0,0,0,0,1,0,0,1) \xrightarrow{1r} (1,1,1,0,0,0,1,1,1,0,1,1,0,0,1,0)$	7,16,17,18	4,6,13,17,18	2^{-23}
$(0,0,0,1,0,1,1,0,0,0,0,0,1,0,1,0) \xrightarrow{1r} (1,1,0,1,1,1,0,1,0,1,0,1,0,0,1,0)$	7,18	4,6,13,15,18	$2^{-17.5}$
$(0,0,0,1,0,1,1,0,0,0,0,0,1,0,1,1) \xrightarrow{1r} (0,0,1,0,0,0,1,0,1,0,1,0,1,1,0,0)$	7,16,17	4,6,13,15,17	2^{-23}
$(0,0,0,1,0,1,1,0,0,0,0,0,1,1,0,0) \xrightarrow{1r} (1,1,0,0,0,0,0,1,0,0,1,1,0,0,1,1)$	7,14,17,18	4,6,13,17,18	2^{-12}
$(0,0,0,1,0,1,1,0,0,0,0,0,1,1,0,1) \xrightarrow{1r} (0,0,1,1,1,1,1,0,1,1,0,0,1,1,0,1)$	7,14,16	4,6,13	$2^{-17.5}$
$(0,0,0,1,0,1,1,0,0,0,0,0,1,1,1,0) \xrightarrow{1r} (0,0,0,0,0,0,0,0,0,0,0,1,1,0,0,1,1)$	7,14,17	4,6,13,15,17	2^{-12}
$(0,0,0,1,0,1,1,0,0,0,0,0,1,1,1,1) \xrightarrow{1r} (1,1,1,1,1,1,1,1,1,1,0,0,1,1,0,1)$	7,14,16,18	4,6,13,15,18	$2^{-17.5}$
$(0,0,0,1,0,1,1,0,0,0,0,1,0,0,0,0) \xrightarrow{1r} (0,0,0,1,0,1,1,1,0,1,0,1,0,0,1,1)$	7,12,17	4,6,17	$2^{-17.5}$
$(0,0,0,1,0,1,1,0,0,0,0,1,0,0,0,1) \xrightarrow{1r} (1,1,1,0,1,0,0,0,1,0,1,0,1,1,0,1)$	7,12,16,18	4,6,18	2^{-12}
$(0,0,0,1,0,1,1,0,0,0,0,1,0,0,1,0) \xrightarrow{1r} (1,1,0,1,0,1,1,0,0,1,0,1,0,0,1,1)$	7,12,17,18	4,6,15,17,18	$2^{-17.5}$
$(0,0,0,1,0,1,1,0,0,0,0,1,0,0,1,1) \xrightarrow{1r} (0,0,1,0,1,0,0,1,1,0,1,0,1,1,0,1)$	7,12,16	4,6,15	2^{-12}
$(0,0,0,1,0,1,1,0,0,0,0,1,0,1,0,0) \xrightarrow{1r} (1,1,0,0,1,0,1,0,0,0,1,0,1,1,0,0)$	7,12,14,18	4,6,18	2^{-1}
$(0,0,0,1,0,1,1,0,0,0,0,1,0,1,0,1) \xrightarrow{1r} (0,0,1,1,0,1,0,1,1,1,0,1,0,0,1,0)$	7,12,14,16,17	4,6,17	$2^{-17.5}$
$(0,0,0,1,0,1,1,0,0,0,0,1,0,1,1,0) \xrightarrow{1r} (0,0,0,0,1,0,1,1,0,0,1,0,1,1,0,0)$	7,12,14	4,6,15	2^{-1}
$(0,0,0,1,0,1,1,0,0,0,0,1,0,1,1,1) \xrightarrow{1r} (1,1,1,1,0,1,0,0,1,1,0,1,0,0,1,0)$	7,12,14,16,17,18	4,6,15,17,18	$2^{-17.5}$
$(0,0,0,1,0,1,1,0,0,0,0,1,1,0,0,0) \xrightarrow{1r} (1,1,0,0,0,0,1,1,0,0,0,1,0,0,1,1)$	7,12,17,18	4,6,13,17,18	2^{-12}
$(0,0,0,1,0,1,1,0,0,0,0,1,1,0,0,1) \xrightarrow{1r} (0,0,1,1,1,1,0,0,1,1,1,0,1,1,0,1)$	7,12,16	4,6,13	$2^{-6.5}$
$(0,0,0,1,0,1,1,0,0,0,0,1,1,0,1,0) \xrightarrow{1r} (0,0,0,0,0,0,1,0,0,0,0,1,0,0,1,1)$	7,12,17	4,6,13,15,17	2^{-12}
$(0,0,0,1,0,1,1,0,0,0,0,1,1,0,1,1) \xrightarrow{1r} (1,1,1,1,1,1,0,1,1,1,1,0,1,1,0,1)$	7,12,16,18	4,6,13,15,18	$2^{-6.5}$
$(0,0,0,1,0,1,1,0,0,0,0,1,1,1,0,0) \xrightarrow{1r} (0,0,0,1,1,1,1,0,0,1,1,0,1,1,0,0)$	7,12,14	4,6,13	$2^{-6.5}$
$(0,0,0,1,0,1,1,0,0,0,0,1,1,1,0,1) \xrightarrow{1r} (1,1,1,0,0,0,0,1,1,0,0,1,0,0,1,0)$	7,12,14,16,17,18	4,6,13,17,18	2^{-23}
$(0,0,0,1,0,1,1,0,0,0,0,1,1,1,1,0) \xrightarrow{1r} (1,1,0,1,1,1,1,1,0,1,1,0,1,1,0,0)$	7,12,14,18	4,6,13,15,18	$2^{-6.5}$
$(0,0,0,1,0,1,1,0,0,0,0,1,1,1,1,1) \xrightarrow{1r} (0,0,1,0,0,0,0,0,1,0,0,1,0,0,1,0)$	7,12,14,16,17	4,6,13,15,17	2^{-23}

Table 0.178 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	7	4,6,11	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	7,16,17,18	4,6,11,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	7,18	4,6,11,15,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	7,16,17	4,6,11,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	7,14,17,18	4,6,11,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	7,14,16	4,6,11	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	7,14,17	4,6,11,15,17	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	7,14,16,18	4,6,11,15,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	7,18	4,6,11,13,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	7,16,17	4,6,11,13,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	7	4,6,11,13,15	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	7,16,17,18	4,6,11,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	7,14,17	4,6,11,13,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	7,14,16,18	4,6,11,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	7,14,17,18	4,6,11,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	7,14,16	4,6,11,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	7,12,17,18	4,6,11,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	7,12,16	4,6,11	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	7,12,17	4,6,11,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	7,12,16,18	4,6,11,15,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	7,12,14	4,6,11	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	7,12,14,16,17,18	4,6,11,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	7,12,14,18	4,6,11,15,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	7,12,14,16,17	4,6,11,15,17	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	7,12,17	4,6,11,13,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	7,12,16,18	4,6,11,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	7,12,17,18	4,6,11,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	7,12,16	4,6,11,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	7,12,14,18	4,6,11,13,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	7,12,14,16,17	4,6,11,13,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	7,12,14	4,6,11,13,15	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	7,12,14,16,17,18	4,6,11,13,15,17,18	2^{-23}

Table 0.179 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(2)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	7,10,17	4,6,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	7,10,16,18	4,6,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	7,10,17,18	4,6,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	7,10,16	4,6,15	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	7,10,14,18	4,6,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	7,10,14,16,17	4,6,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	7,10,14	4,6,15	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	7,10,14,16,17,18	4,6,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	7,10,17,18	4,6,13,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	7,10,16	4,6,13	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	7,10,17	4,6,13,15,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	7,10,16,18	4,6,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	7,10,14	4,6,13	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	7,10,14,16,17,18	4,6,13,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	7,10,14,18	4,6,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	7,10,14,16,17	4,6,13,15,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	7,10,12,18	4,6,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	7,10,12,16,17	4,6,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	7,10,12	4,6,15	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	7,10,12,16,17,18	4,6,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	7,10,12,14,17	4,6,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	7,10,12,14,16,18	4,6,18	2^{-34}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	7,10,12,14,17,18	4,6,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	7,10,12,14,16	4,6,15	2^{-34}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	7,10,12	4,6,13	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	7,10,12,16,17,18	4,6,13,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	7,10,12,18	4,6,13,15,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	7,10,12,16,17	4,6,13,15,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	7,10,12,14,17,18	4,6,13,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	7,10,12,14,16	4,6,13	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	7,10,12,14,17	4,6,13,15,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	7,10,12,14,16,18	4,6,13,15,18	$2^{-28.5}$

Table 0.180 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	7,10,17,18	4,6,11,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	7,10,16	4,6,11	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	7,10,17	4,6,11,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	7,10,16,18	4,6,11,15,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	7,10,14	4,6,11	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	7,10,14,16,17,18	4,6,11,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	7,10,14,18	4,6,11,15,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	7,10,14,16,17	4,6,11,15,17	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	7,10,17	4,6,11,13,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	7,10,16,18	4,6,11,13,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	7,10,17,18	4,6,11,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	7,10,16	4,6,11,13,15	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	7,10,14,18	4,6,11,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	7,10,14,16,17	4,6,11,13,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	7,10,14	4,6,11,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	7,10,14,16,17,18	4,6,11,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	7,10,12	4,6,11	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	7,10,12,16,17,18	4,6,11,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	7,10,12,18	4,6,11,15,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	7,10,12,16,17	4,6,11,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	7,10,12,14,17,18	4,6,11,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	7,10,12,14,16	4,6,11	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	7,10,12,14,17	4,6,11,15,17	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	7,10,12,14,16,18	4,6,11,15,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	7,10,12,18	4,6,11,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	7,10,12,16,17	4,6,11,13,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	7,10,12	4,6,11,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	7,10,12,16,17,18	4,6,11,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	7,10,12,14,17	4,6,11,13,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	7,10,12,14,16,18	4,6,11,13,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	7,10,12,14,17,18	4,6,11,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	7,10,12,14,16	4,6,11,13,15	$2^{-28.5}$

Table 0.181 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	7	4,6,9	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	7,16,17,18	4,6,9,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	7,18	4,6,9,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	7,16,17	4,6,9,15,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	7,14,17,18	4,6,9,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	7,14,16	4,6,9	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	7,14,17	4,6,9,15,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	7,14,16,18	4,6,9,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	7,18	4,6,9,13,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	7,16,17	4,6,9,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	7	4,6,9,13,15	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	7,16,17,18	4,6,9,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	7,14,17	4,6,9,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	7,14,16,18	4,6,9,13,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	7,14,17,18	4,6,9,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	7,14,16	4,6,9,13,15	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	7,12,17,18	4,6,9,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	7,12,16	4,6,9	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	7,12,17	4,6,9,15,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	7,12,16,18	4,6,9,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	7,12,14	4,6,9	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	7,12,14,16,17,18	4,6,9,17,18	2^{-34}
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	7,12,14,18	4,6,9,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	7,12,14,16,17	4,6,9,15,17	2^{-34}
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	7,12,17	4,6,9,13,17	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	7,12,16,18	4,6,9,13,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	7,12,17,18	4,6,9,13,15,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	7,12,16	4,6,9,13,15	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	7,12,14,18	4,6,9,13,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	7,12,14,16,17	4,6,9,13,17	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	7,12,14	4,6,9,13,15	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	7,12,14,16,17,18	4,6,9,13,15,17,18	$2^{-28.5}$

Table 0.182 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,1,0,1,1,0,1,0,1,0,0,0,0,0) \xrightarrow{1r} (1,0,0,1,1,0,0,1,0,0,0,0,1,0,0,0)$	7,18	4,6,9,11,18	$2^{-17.5}$
$(0,0,0,1,0,1,1,0,1,0,1,0,0,0,0,1) \xrightarrow{1r} (0,1,1,0,0,1,1,0,1,1,1,1,0,1,1,0)$	7,16,17	4,6,9,11,17	2^{-23}
$(0,0,0,1,0,1,1,0,1,0,1,0,0,0,1,0) \xrightarrow{1r} (0,1,0,1,1,0,0,0,0,0,0,0,0,1,0,0)$	7	4,6,9,11,15	$2^{-17.5}$
$(0,0,0,1,0,1,1,0,1,0,1,0,0,0,1,1) \xrightarrow{1r} (1,0,1,0,0,1,1,1,1,1,1,1,0,1,1,0)$	7,16,17,18	4,6,9,11,15,17,18	2^{-23}
$(0,0,0,1,0,1,1,0,1,0,1,0,0,1,0,0) \xrightarrow{1r} (0,1,0,0,0,1,0,0,0,1,1,1,0,1,1,1)$	7,14,17	4,6,9,11,17	2^{-23}
$(0,0,0,1,0,1,1,0,1,0,1,0,0,1,0,1) \xrightarrow{1r} (1,0,1,1,0,1,1,1,0,0,0,1,0,0,1,1)$	7,14,16,18	4,6,9,11,18	$2^{-28.5}$
$(0,0,0,1,0,1,1,0,1,0,1,0,0,1,1,0) \xrightarrow{1r} (1,0,0,0,0,1,0,1,0,1,1,1,0,1,1,1)$	7,14,17,18	4,6,9,11,15,17,18	2^{-23}
$(0,0,0,1,0,1,1,0,1,0,1,0,0,1,1,1) \xrightarrow{1r} (0,1,1,1,0,1,0,1,0,0,0,1,0,0,1,0)$	7,14,16	4,6,9,11,15	$2^{-28.5}$
$(0,0,0,1,0,1,1,0,1,0,1,0,1,0,0,0) \xrightarrow{1r} (0,1,0,0,1,1,0,1,0,1,0,0,1,0,0,0)$	7	4,6,9,11,13	2^{-23}
$(0,0,0,1,0,1,1,0,1,0,1,0,1,0,0,1) \xrightarrow{1r} (1,0,1,1,0,0,1,0,1,0,1,0,1,1,0,1)$	7,16,17,18	4,6,9,11,13,17,18	$2^{-28.5}$
$(0,0,0,1,0,1,1,0,1,0,1,0,1,0,1,0) \xrightarrow{1r} (1,0,0,0,1,1,0,0,0,1,0,0,1,0,0,0)$	7,18	4,6,9,11,13,15,18	2^{-23}
$(0,0,0,1,0,1,1,0,1,0,1,0,1,0,1,1) \xrightarrow{1r} (0,1,1,1,0,0,1,1,1,0,1,1,0,1,1,0)$	7,16,17	4,6,9,11,13,15,17	$2^{-28.5}$
$(0,0,0,1,0,1,1,0,1,0,1,0,1,1,0,0) \xrightarrow{1r} (1,0,0,1,0,0,0,0,0,0,0,1,1,0,1,1)$	7,14,17,18	4,6,9,11,13,17,18	$2^{-17.5}$
$(0,0,0,1,0,1,1,0,1,0,1,0,1,1,0,1) \xrightarrow{1r} (0,1,1,0,1,1,1,1,1,1,0,0,1,0,0,1)$	7,14,16	4,6,9,11,13	2^{-23}
$(0,0,0,1,0,1,1,0,1,0,1,0,1,1,1,0) \xrightarrow{1r} (0,1,0,1,0,0,0,1,0,0,1,1,0,1,1,1)$	7,14,17	4,6,9,11,13,15,17	$2^{-17.5}$
$(0,0,0,1,0,1,1,0,1,0,1,0,1,1,1,1) \xrightarrow{1r} (1,0,1,0,1,1,1,0,1,1,0,0,1,0,0,1)$	7,14,16,18	4,6,9,11,13,15,18	2^{-23}
$(0,0,0,1,0,1,1,0,1,0,1,0,0,0,0,0) \xrightarrow{1r} (0,1,0,0,0,1,1,0,0,1,0,1,0,1,1,1)$	7,12,17	4,6,9,11,17	2^{-23}
$(0,0,0,1,0,1,1,0,1,0,1,0,0,0,0,1) \xrightarrow{1r} (1,0,1,1,1,0,0,1,1,0,1,0,1,0,0,1)$	7,12,16,18	4,6,9,11,18	$2^{-17.5}$
$(0,0,0,1,0,1,1,0,1,0,1,0,0,0,1,0) \xrightarrow{1r} (1,0,0,0,0,1,1,1,0,1,0,1,0,1,1,1)$	7,12,17,18	4,6,9,11,15,17,18	2^{-23}
$(0,0,0,1,0,1,1,0,1,0,1,0,0,0,1,1) \xrightarrow{1r} (0,1,1,1,1,0,0,0,1,0,1,0,1,0,0,1)$	7,12,16	4,6,9,11,15	$2^{-17.5}$
$(0,0,0,1,0,1,1,0,1,0,1,0,1,0,0,0) \xrightarrow{1r} (1,0,0,1,1,0,1,1,0,0,1,0,1,0,0,0)$	7,12,14,18	4,6,9,11,18	$2^{-6.5}$
$(0,0,0,1,0,1,1,0,1,0,1,0,1,0,1,0) \xrightarrow{1r} (0,1,1,0,0,1,0,0,1,1,0,1,0,1,1,0)$	7,12,14,16,17	4,6,9,11,17	2^{-23}
$(0,0,0,1,0,1,1,0,1,0,1,0,1,0,1,1) \xrightarrow{1r} (0,1,0,1,1,0,1,0,0,0,1,0,1,0,0,0)$	7,12,14	4,6,9,11,15	$2^{-6.5}$
$(0,0,0,1,0,1,1,0,1,0,1,0,1,1,1,1) \xrightarrow{1r} (1,0,1,0,0,1,0,1,1,1,0,1,0,1,1,0)$	7,12,14,16,17,18	4,6,9,11,15,17,18	2^{-23}
$(0,0,0,1,0,1,1,0,1,0,1,0,1,1,0,0) \xrightarrow{1r} (1,0,0,1,0,0,1,0,0,0,0,1,0,1,1,1)$	7,12,17,18	4,6,9,11,13,17,18	$2^{-17.5}$
$(0,0,0,1,0,1,1,0,1,0,1,0,1,1,0,0) \xrightarrow{1r} (0,1,1,0,1,1,0,1,1,1,1,0,1,0,0,1)$	7,12,16	4,6,9,11,13	2^{-12}
$(0,0,0,1,0,1,1,0,1,0,1,0,1,1,0,1) \xrightarrow{1r} (0,1,0,1,0,0,1,1,0,0,0,1,0,1,1,1)$	7,12,17	4,6,9,11,13,15,17	$2^{-17.5}$
$(0,0,0,1,0,1,1,0,1,0,1,0,1,1,0,1) \xrightarrow{1r} (1,0,1,0,1,1,0,0,1,1,1,0,1,0,0,1)$	7,12,16,18	4,6,9,11,13,15,18	2^{-12}
$(0,0,0,1,0,1,1,0,1,0,1,1,1,1,0,0) \xrightarrow{1r} (0,1,0,0,1,1,1,1,0,1,1,0,1,0,0,0)$	7,12,14	4,6,9,11,13	2^{-12}
$(0,0,0,1,0,1,1,0,1,0,1,1,1,1,0,1) \xrightarrow{1r} (1,0,1,1,0,0,0,0,1,0,0,1,0,1,1,0)$	7,12,14,16,17,18	4,6,9,11,13,17,18	$2^{-28.5}$
$(0,0,0,1,0,1,1,0,1,0,1,1,1,1,1,0) \xrightarrow{1r} (1,0,0,0,1,1,1,0,0,1,1,0,1,0,0,0)$	7,12,14,18	4,6,9,11,13,15,18	2^{-12}
$(0,0,0,1,0,1,1,0,1,0,1,1,1,1,1,1) \xrightarrow{1r} (0,1,1,1,0,0,0,1,1,0,0,1,0,1,1,0)$	7,12,14,16,17	4,6,9,11,13,15,17	$2^{-28.5}$

Table 0.183 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	7,10,17,18	4,6,9,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	7,10,16	4,6,9	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	7,10,17	4,6,9,15,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	7,10,16,18	4,6,9,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	7,10,14	4,6,9	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	7,10,14,16,17,18	4,6,9,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	7,10,14,18	4,6,9,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	7,10,14,16,17	4,6,9,15,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	7,10,17	4,6,9,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	7,10,16,18	4,6,9,13,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	7,10,17,18	4,6,9,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	7,10,16	4,6,9,13,15	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	7,10,14,18	4,6,9,13,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	7,10,14,16,17	4,6,9,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	7,10,14	4,6,9,13,15	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	7,10,14,16,17,18	4,6,9,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	7,10,12	4,6,9	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	7,10,12,16,17,18	4,6,9,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	7,10,12,18	4,6,9,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	7,10,12,16,17	4,6,9,15,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	7,10,12,14,17,18	4,6,9,17,18	2^{-1}
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	7,10,12,14,16	4,6,9	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	7,10,12,14,17	4,6,9,15,17	2^{-1}
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	7,10,12,14,16,18	4,6,9,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	7,10,12,18	4,6,9,13,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	7,10,12,16,17	4,6,9,13,17	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	7,10,12	4,6,9,13,15	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	7,10,12,16,17,18	4,6,9,13,15,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	7,10,12,14,17	4,6,9,13,17	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	7,10,12,14,16,18	4,6,9,13,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	7,10,12,14,17,18	4,6,9,13,15,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	7,10,12,14,16	4,6,9,13,15	2^{-23}

Table 0.184 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,1,0,1,1,0,1,1,1,0,0,0,0,0) \xrightarrow{1r} (0,1,1,0,1,1,0,0,0,1,0,1,1,1,1,1)$	7,10,17	4,6,9,11,17	2^{-12}
$(0,0,0,1,0,1,1,0,1,1,1,0,0,0,0,1) \xrightarrow{1r} (1,0,0,1,0,0,1,1,1,0,1,0,0,0,0,1)$	7,10,16,18	4,6,9,11,18	$2^{-17.5}$
$(0,0,0,1,0,1,1,0,1,1,1,0,0,0,1,0) \xrightarrow{1r} (1,0,1,0,1,1,0,1,0,1,0,1,1,1,1,1)$	7,10,17,18	4,6,9,11,15,17,18	2^{-12}
$(0,0,0,1,0,1,1,0,1,1,1,0,0,0,1,1) \xrightarrow{1r} (0,1,0,1,0,0,1,0,1,0,1,0,0,0,0,1)$	7,10,16	4,6,9,11,15	$2^{-17.5}$
$(0,0,0,1,0,1,1,0,1,1,1,0,0,1,0,0) \xrightarrow{1r} (1,0,1,1,0,0,0,1,0,0,1,0,0,0,0,0)$	7,10,14,18	4,6,9,11,18	$2^{-6.5}$
$(0,0,0,1,0,1,1,0,1,1,1,0,0,1,0,1) \xrightarrow{1r} (0,1,0,0,1,1,1,0,1,1,0,1,1,1,1,0)$	7,10,14,16,17	4,6,9,11,17	2^{-12}
$(0,0,0,1,0,1,1,0,1,1,1,0,0,1,1,0) \xrightarrow{1r} (0,1,1,1,0,0,0,0,0,0,1,0,0,0,0,0)$	7,10,14	4,6,9,11,15	$2^{-6.5}$
$(0,0,0,1,0,1,1,0,1,1,1,0,0,1,1,1) \xrightarrow{1r} (1,0,0,0,1,1,1,1,1,0,1,1,1,1,0)$	7,10,14,16,17,18	4,6,9,11,15,17,18	2^{-12}
$(0,0,0,1,0,1,1,0,1,1,1,0,1,0,0,0) \xrightarrow{1r} (1,0,1,1,1,0,0,0,0,0,0,1,1,1,1,1)$	7,10,17,18	4,6,9,11,13,17,18	$2^{-6.5}$
$(0,0,0,1,0,1,1,0,1,1,1,0,1,0,0,1) \xrightarrow{1r} (0,1,0,0,0,1,1,1,1,1,0,0,0,0,0,1)$	7,10,16	4,6,9,11,13	2^{-12}
$(0,0,0,1,0,1,1,0,1,1,1,0,1,0,1,0) \xrightarrow{1r} (0,1,1,1,1,0,0,1,0,0,0,1,1,1,1,1)$	7,10,17	4,6,9,11,13,15,17	$2^{-6.5}$
$(0,0,0,1,0,1,1,0,1,1,1,0,1,0,1,1) \xrightarrow{1r} (1,0,0,0,0,1,1,0,1,1,1,0,0,0,0,1)$	7,10,16,18	4,6,9,11,13,15,18	2^{-12}
$(0,0,0,1,0,1,1,0,1,1,1,0,1,1,0,0) \xrightarrow{1r} (0,1,1,0,0,1,0,1,0,1,1,0,0,0,0,0)$	7,10,14	4,6,9,11,13	2^{-12}
$(0,0,0,1,0,1,1,0,1,1,1,0,1,1,0,1) \xrightarrow{1r} (1,0,0,1,1,0,1,0,1,0,0,1,1,1,1,0)$	7,10,14,16,17,18	4,6,9,11,13,17,18	$2^{-17.5}$
$(0,0,0,1,0,1,1,0,1,1,1,0,1,1,1,0) \xrightarrow{1r} (1,0,1,0,0,1,0,0,0,1,1,0,0,0,0,0)$	7,10,14,18	4,6,9,11,13,15,18	2^{-12}
$(0,0,0,1,0,1,1,0,1,1,1,0,1,1,1,1) \xrightarrow{1r} (0,1,0,1,1,0,1,1,1,0,0,1,1,1,1,0)$	7,10,14,16,17	4,6,9,11,13,15,17	$2^{-17.5}$
$(0,0,0,1,0,1,1,0,1,1,1,1,0,0,0,0) \xrightarrow{1r} (1,0,1,1,0,0,1,1,0,0,0,0,0,0,0,0)$	7,10,12,18	4,6,9,11,18	$2^{-17.5}$
$(0,0,0,1,0,1,1,0,1,1,1,1,0,0,0,1) \xrightarrow{1r} (0,1,0,0,1,1,0,0,1,1,1,1,1,1,1,0)$	7,10,12,16,17	4,6,9,11,17	2^{-12}
$(0,0,0,1,0,1,1,0,1,1,1,1,0,0,1,0) \xrightarrow{1r} (0,1,1,1,0,0,1,0,0,0,0,0,0,0,0,0)$	7,10,12	4,6,9,11,15	$2^{-17.5}$
$(0,0,0,1,0,1,1,0,1,1,1,1,0,0,1,1) \xrightarrow{1r} (1,0,0,0,1,1,0,1,1,1,1,1,1,1,0)$	7,10,12,16,17,18	4,6,9,11,15,17,18	2^{-12}
$(0,0,0,1,0,1,1,0,1,1,1,1,0,1,0,0) \xrightarrow{1r} (0,1,1,0,1,1,1,0,0,1,1,1,1,1,1,1)$	7,10,12,14,17	4,6,9,11,17	2^{-12}
$(0,0,0,1,0,1,1,0,1,1,1,1,0,1,0,1) \xrightarrow{1r} (1,0,0,1,0,0,0,1,1,0,0,0,0,0,0,1)$	7,10,12,14,16,18	4,6,9,11,18	$2^{-28.5}$
$(0,0,0,1,0,1,1,0,1,1,1,1,0,1,1,0) \xrightarrow{1r} (1,0,1,0,1,1,1,1,0,1,1,1,1,1,1,1)$	7,10,12,14,17,18	4,6,9,11,15,17,18	2^{-12}
$(0,0,0,1,0,1,1,0,1,1,1,1,0,1,1,1) \xrightarrow{1r} (0,1,0,1,0,0,0,0,1,0,0,0,0,0,0,1)$	7,10,12,14,16	4,6,9,11,15	$2^{-28.5}$
$(0,0,0,1,0,1,1,0,1,1,1,1,1,0,0,0) \xrightarrow{1r} (0,1,1,0,0,1,1,1,0,1,0,0,0,0,0,0)$	7,10,12	4,6,9,11,13	2^{-23}
$(0,0,0,1,0,1,1,0,1,1,1,1,1,0,0,1) \xrightarrow{1r} (1,0,0,1,1,0,0,0,1,0,1,1,1,1,1,0)$	7,10,12,16,17,18	4,6,9,11,13,17,18	$2^{-17.5}$
$(0,0,0,1,0,1,1,0,1,1,1,1,1,0,1,0) \xrightarrow{1r} (1,0,1,0,0,1,1,0,0,1,0,0,0,0,0,0)$	7,10,12,18	4,6,9,11,13,15,18	2^{-23}
$(0,0,0,1,0,1,1,0,1,1,1,1,1,0,1,1) \xrightarrow{1r} (0,1,0,1,1,0,0,1,1,0,1,1,1,1,1,0)$	7,10,12,16,17	4,6,9,11,13,15,17	$2^{-17.5}$
$(0,0,0,1,0,1,1,0,1,1,1,1,1,1,0,0) \xrightarrow{1r} (1,0,1,1,1,0,1,0,0,0,1,1,1,1,1,1)$	7,10,12,14,17,18	4,6,9,11,13,17,18	$2^{-6.5}$
$(0,0,0,1,0,1,1,0,1,1,1,1,1,1,0,1) \xrightarrow{1r} (0,1,0,0,0,1,0,1,1,1,0,0,0,0,0,1)$	7,10,12,14,16	4,6,9,11,13	2^{-23}
$(0,0,0,1,0,1,1,0,1,1,1,1,1,1,1,0) \xrightarrow{1r} (0,1,1,1,0,1,1,0,0,1,1,1,1,1,1,1)$	7,10,12,14,17	4,6,9,11,13,15,17	$2^{-6.5}$
$(0,0,0,1,0,1,1,0,1,1,1,1,1,1,1,1) \xrightarrow{1r} (1,0,0,0,0,1,0,0,1,1,0,0,0,0,0,1)$	7,10,12,14,16,18	4,6,9,11,13,15,18	2^{-23}

Table 0.185 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	7,17	4,6,8,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	7,16,18	4,6,8,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	7,17,18	4,6,8,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	7,16	4,6,8,15	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	7,14,18	4,6,8,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	7,14,16,17	4,6,8,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	7,14	4,6,8,15	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	7,14,16,17,18	4,6,8,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	7,17,18	4,6,8,13,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	7,16	4,6,8,13	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	7,17	4,6,8,13,15,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	7,16,18	4,6,8,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	7,14	4,6,8,13	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	7,14,16,17,18	4,6,8,13,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	7,14,18	4,6,8,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	7,14,16,17	4,6,8,13,15,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	7,12,18	4,6,8,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	7,12,16,17	4,6,8,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	7,12	4,6,8,15	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	7,12,16,17,18	4,6,8,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	7,12,14,17	4,6,8,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	7,12,14,16,18	4,6,8,18	2^{-1}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	7,12,14,17,18	4,6,8,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	7,12,14,16	4,6,8,15	2^{-1}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	7,12	4,6,8,13	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	7,12,16,17,18	4,6,8,13,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	7,12,18	4,6,8,13,15,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	7,12,16,17	4,6,8,13,15,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	7,12,14,17,18	4,6,8,13,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	7,12,14,16	4,6,8,13	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	7,12,14,17	4,6,8,13,15,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	7,12,14,16,18	4,6,8,13,15,18	$2^{-6.5}$

Table 0.186 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,1,0,1,1,1,0,0,1,0,0,0,0,0) \xrightarrow{1r} (1,1,1,1,0,0,1,1,1,0,1,0,0,0,0,1)$	7,17,18	4,6,8,11,17,18	$2^{-17.5}$
$(0,0,0,1,0,1,1,1,0,0,1,0,0,0,0,1) \xrightarrow{1r} (0,0,0,0,1,1,0,0,0,1,0,1,1,1,1,1)$	7,16	4,6,8,11	2^{-12}
$(0,0,0,1,0,1,1,1,0,0,1,0,0,0,1,0) \xrightarrow{1r} (0,0,1,1,0,0,1,0,1,0,1,0,0,0,0,1)$	7,17	4,6,8,11,15,17	$2^{-17.5}$
$(0,0,0,1,0,1,1,1,0,0,1,0,0,0,1,1) \xrightarrow{1r} (1,1,0,0,1,1,0,1,0,1,0,1,1,1,1,1)$	7,16,18	4,6,8,11,15,18	2^{-12}
$(0,0,0,1,0,1,1,1,0,0,1,0,0,1,0,0) \xrightarrow{1r} (0,0,1,0,1,1,1,0,1,1,0,1,1,1,1,0)$	7,14	4,6,8,11	2^{-12}
$(0,0,0,1,0,1,1,1,0,0,1,0,0,1,0,1) \xrightarrow{1r} (1,1,0,1,0,0,0,1,0,0,1,0,0,0,0,0)$	7,14,16,17,18	4,6,8,11,17,18	$2^{-6.5}$
$(0,0,0,1,0,1,1,1,0,0,1,0,0,1,1,0) \xrightarrow{1r} (1,1,1,0,1,1,1,1,1,1,0,1,1,1,1,0)$	7,14,18	4,6,8,11,15,18	2^{-12}
$(0,0,0,1,0,1,1,1,0,0,1,0,0,1,1,1) \xrightarrow{1r} (0,0,0,1,0,0,0,0,0,0,1,0,0,0,0,0)$	7,14,16,17	4,6,8,11,15,17	$2^{-6.5}$
$(0,0,0,1,0,1,1,1,0,0,1,0,1,0,0,0) \xrightarrow{1r} (0,0,1,0,0,1,1,1,1,1,1,0,0,0,0,1)$	7,17	4,6,8,11,13,17	2^{-12}
$(0,0,0,1,0,1,1,1,0,0,1,0,1,0,0,1) \xrightarrow{1r} (1,1,0,1,1,0,0,0,0,0,0,1,1,1,1,1)$	7,16,18	4,6,8,11,13,18	$2^{-6.5}$
$(0,0,0,1,0,1,1,1,0,0,1,0,1,0,1,0) \xrightarrow{1r} (1,1,1,0,0,1,1,0,1,1,1,1,0,0,0,1)$	7,17,18	4,6,8,11,13,15,17,18	2^{-12}
$(0,0,0,1,0,1,1,1,0,0,1,0,1,0,1,1) \xrightarrow{1r} (0,0,0,1,1,0,0,1,0,0,0,1,1,1,1,1)$	7,16	4,6,8,11,13,15	$2^{-6.5}$
$(0,0,0,1,0,1,1,1,0,0,1,0,1,1,0,0) \xrightarrow{1r} (1,1,1,1,1,0,1,0,1,0,0,1,1,1,1,0)$	7,14,18	4,6,8,11,13,18	$2^{-17.5}$
$(0,0,0,1,0,1,1,1,0,0,1,0,1,1,0,1) \xrightarrow{1r} (0,0,0,0,0,1,0,1,0,1,1,0,0,0,0,0)$	7,14,16,17	4,6,8,11,13,17	2^{-12}
$(0,0,0,1,0,1,1,1,0,0,1,0,1,1,1,0) \xrightarrow{1r} (0,0,1,1,1,0,1,1,1,0,0,1,1,1,1,0)$	7,14	4,6,8,11,13,15	$2^{-17.5}$
$(0,0,0,1,0,1,1,1,0,0,1,0,1,1,1,1) \xrightarrow{1r} (1,1,0,0,0,1,0,0,0,1,1,0,0,0,0,0)$	7,14,16,17,18	4,6,8,11,13,15,17,18	2^{-12}
$(0,0,0,1,0,1,1,1,0,0,1,1,0,0,0,0) \xrightarrow{1r} (0,0,1,0,1,1,0,0,1,1,1,1,1,1,1,0)$	7,12	4,6,8,11	2^{-12}
$(0,0,0,1,0,1,1,1,0,0,1,1,0,0,0,1) \xrightarrow{1r} (1,1,0,1,0,0,1,1,0,0,0,0,0,0,0,0)$	7,12,16,17,18	4,6,8,11,17,18	$2^{-17.5}$
$(0,0,0,1,0,1,1,1,0,0,1,1,0,0,1,0) \xrightarrow{1r} (1,1,1,0,1,1,0,1,1,1,1,1,1,1,1,0)$	7,12,18	4,6,8,11,15,18	2^{-12}
$(0,0,0,1,0,1,1,1,0,0,1,1,0,0,1,1) \xrightarrow{1r} (0,0,0,1,0,0,1,0,0,0,0,0,0,0,0,0)$	7,12,16,17	4,6,8,11,15,17	$2^{-17.5}$
$(0,0,0,1,0,1,1,1,0,0,1,1,0,0,1,0) \xrightarrow{1r} (1,1,1,1,0,0,0,1,1,0,0,0,0,0,0,1)$	7,12,14,17,18	4,6,8,11,17,18	$2^{-28.5}$
$(0,0,0,1,0,1,1,1,0,0,1,1,0,0,1,0) \xrightarrow{1r} (0,0,0,0,1,1,1,0,0,1,1,1,1,1,1,1)$	7,12,14,16	4,6,8,11	2^{-12}
$(0,0,0,1,0,1,1,1,0,0,1,1,0,0,1,1) \xrightarrow{1r} (0,0,1,1,0,0,0,0,1,0,0,0,0,0,0,1)$	7,12,14,17	4,6,8,11,15,17	$2^{-28.5}$
$(0,0,0,1,0,1,1,1,0,0,1,1,0,0,1,1) \xrightarrow{1r} (1,1,0,0,1,1,1,1,0,1,1,1,1,1,1,1)$	7,12,14,16,18	4,6,8,11,15,18	2^{-12}
$(0,0,0,1,0,1,1,1,0,0,1,1,1,0,0,0) \xrightarrow{1r} (1,1,1,1,1,0,0,0,1,0,1,1,1,1,1,0)$	7,12,18	4,6,8,11,13,18	$2^{-17.5}$
$(0,0,0,1,0,1,1,1,0,0,1,1,1,0,0,1) \xrightarrow{1r} (0,0,0,0,0,1,1,1,0,1,0,0,0,0,0,0)$	7,12,16,17	4,6,8,11,13,17	2^{-23}
$(0,0,0,1,0,1,1,1,0,0,1,1,1,0,1,0) \xrightarrow{1r} (0,0,1,1,1,0,0,1,1,0,1,1,1,1,1,0)$	7,12	4,6,8,11,13,15	$2^{-17.5}$
$(0,0,0,1,0,1,1,1,0,0,1,1,1,0,1,1) \xrightarrow{1r} (1,1,0,0,0,1,1,0,0,1,0,0,0,0,0,0)$	7,12,16,17,18	4,6,8,11,13,15,17,18	2^{-23}
$(0,0,0,1,0,1,1,1,0,0,1,1,1,1,0,0) \xrightarrow{1r} (0,0,1,0,0,1,0,1,1,1,0,0,0,0,0,1)$	7,12,14,17	4,6,8,11,13,17	2^{-23}
$(0,0,0,1,0,1,1,1,0,0,1,1,1,1,0,1) \xrightarrow{1r} (1,1,0,1,1,0,1,0,0,0,1,1,1,1,1,1)$	7,12,14,16,18	4,6,8,11,13,18	$2^{-6.5}$
$(0,0,0,1,0,1,1,1,0,0,1,1,1,1,1,0) \xrightarrow{1r} (1,1,1,0,0,1,0,0,1,1,0,0,0,0,0,1)$	7,12,14,17,18	4,6,8,11,13,15,17,18	2^{-23}
$(0,0,0,1,0,1,1,1,0,0,1,1,1,1,1,1) \xrightarrow{1r} (0,0,0,1,1,0,1,1,0,0,1,1,1,1,1,1)$	7,12,14,16	4,6,8,11,13,15	$2^{-6.5}$

Table 0.187 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	7,10,18	4,6,8,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	7,10,16,17	4,6,8,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	7,10	4,6,8,15	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	7,10,16,17,18	4,6,8,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	7,10,14,17	4,6,8,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	7,10,14,16,18	4,6,8,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	7,10,14,17,18	4,6,8,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	7,10,14,16	4,6,8,15	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	7,10	4,6,8,13	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	7,10,16,17,18	4,6,8,13,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	7,10,18	4,6,8,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	7,10,16,17	4,6,8,13,15,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	7,10,14,17,18	4,6,8,13,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	7,10,14,16	4,6,8,13	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	7,10,14,17	4,6,8,13,15,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	7,10,14,16,18	4,6,8,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	7,10,12,17	4,6,8,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	7,10,12,16,18	4,6,8,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	7,10,12,17,18	4,6,8,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	7,10,12,16	4,6,8,15	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	7,10,12,14,18	4,6,8,18	2^{-34}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	7,10,12,14,16,17	4,6,8,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	7,10,12,14	4,6,8,15	2^{-34}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	7,10,12,14,16,17,18	4,6,8,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	7,10,12,17,18	4,6,8,13,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	7,10,12,16	4,6,8,13	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	7,10,12,17	4,6,8,13,15,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	7,10,12,16,18	4,6,8,13,15,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	7,10,12,14	4,6,8,13	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	7,10,12,14,16,17,18	4,6,8,13,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	7,10,12,14,18	4,6,8,13,15,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	7,10,12,14,16,17	4,6,8,13,15,17	2^{-12}

Table 0.188 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	7,10	4,6,8,11	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	7,10,16,17,18	4,6,8,11,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	7,10,18	4,6,8,11,15,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	7,10,16,17	4,6,8,11,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	7,10,14,17,18	4,6,8,11,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	7,10,14,16	4,6,8,11	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	7,10,14,17	4,6,8,11,15,17	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	7,10,14,16,18	4,6,8,11,15,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	7,10,18	4,6,8,11,13,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	7,10,16,17	4,6,8,11,13,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	7,10	4,6,8,11,13,15	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	7,10,16,17,18	4,6,8,11,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	7,10,14,17	4,6,8,11,13,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	7,10,14,16,18	4,6,8,11,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	7,10,14,17,18	4,6,8,11,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	7,10,14,16	4,6,8,11,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	7,10,12,17,18	4,6,8,11,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	7,10,12,16	4,6,8,11	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	7,10,12,17	4,6,8,11,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	7,10,12,16,18	4,6,8,11,15,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	7,10,12,14	4,6,8,11	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	7,10,12,14,16,17,18	4,6,8,11,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	7,10,12,14,18	4,6,8,11,15,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	7,10,12,14,16,17	4,6,8,11,15,17	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	7,10,12,17	4,6,8,11,13,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	7,10,12,16,18	4,6,8,11,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	7,10,12,17,18	4,6,8,11,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	7,10,12,16	4,6,8,11,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	7,10,12,14,18	4,6,8,11,13,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	7,10,12,14,16,17	4,6,8,11,13,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	7,10,12,14	4,6,8,11,13,15	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	7,10,12,14,16,17,18	4,6,8,11,13,15,17,18	2^{-12}

Table 0.189 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	7,17,18	4,6,8,9,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	7,16	4,6,8,9	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	7,17	4,6,8,9,15,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	7,16,18	4,6,8,9,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	7,14	4,6,8,9	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	7,14,16,17,18	4,6,8,9,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	7,14,18	4,6,8,9,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	7,14,16,17	4,6,8,9,15,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	7,17	4,6,8,9,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	7,16,18	4,6,8,9,13,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	7,17,18	4,6,8,9,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	7,16	4,6,8,9,13,15	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	7,14,18	4,6,8,9,13,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	7,14,16,17	4,6,8,9,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	7,14	4,6,8,9,13,15	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	7,14,16,17,18	4,6,8,9,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	7,12	4,6,8,9	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	7,12,16,17,18	4,6,8,9,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	7,12,18	4,6,8,9,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	7,12,16,17	4,6,8,9,15,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	7,12,14,17,18	4,6,8,9,17,18	2^{-34}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	7,12,14,16	4,6,8,9	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	7,12,14,17	4,6,8,9,15,17	2^{-34}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	7,12,14,16,18	4,6,8,9,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	7,12,18	4,6,8,9,13,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	7,12,16,17	4,6,8,9,13,17	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	7,12	4,6,8,9,13,15	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	7,12,16,17,18	4,6,8,9,13,15,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	7,12,14,17	4,6,8,9,13,17	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	7,12,14,16,18	4,6,8,9,13,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	7,12,14,17,18	4,6,8,9,13,15,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	7,12,14,16	4,6,8,9,13,15	2^{-12}

Table 0.190 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	7,17	4,6,8,9,11,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	7,16,18	4,6,8,9,11,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	7,17,18	4,6,8,9,11,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	7,16	4,6,8,9,11,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	7,14,18	4,6,8,9,11,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	7,14,16,17	4,6,8,9,11,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	7,14	4,6,8,9,11,15	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	7,14,16,17,18	4,6,8,9,11,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	7,17,18	4,6,8,9,11,13,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	7,16	4,6,8,9,11,13	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	7,17	4,6,8,9,11,13,15,17	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	7,16,18	4,6,8,9,11,13,15,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	7,14	4,6,8,9,11,13	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	7,14,16,17,18	4,6,8,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	7,14,18	4,6,8,9,11,13,15,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	7,14,16,17	4,6,8,9,11,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	7,12,18	4,6,8,9,11,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	7,12,16,17	4,6,8,9,11,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	7,12	4,6,8,9,11,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	7,12,16,17,18	4,6,8,9,11,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	7,12,14,17	4,6,8,9,11,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	7,12,14,16,18	4,6,8,9,11,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	7,12,14,17,18	4,6,8,9,11,15,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	7,12,14,16	4,6,8,9,11,15	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	7,12	4,6,8,9,11,13	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	7,12,16,17,18	4,6,8,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	7,12,18	4,6,8,9,11,13,15,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	7,12,16,17	4,6,8,9,11,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	7,12,14,17,18	4,6,8,9,11,13,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	7,12,14,16	4,6,8,9,11,13	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	7,12,14,17	4,6,8,9,11,13,15,17	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	7,12,14,16,18	4,6,8,9,11,13,15,18	2^{-12}

Table 0.191 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	7,10	4,6,8,9	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	7,10,16,17,18	4,6,8,9,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	7,10,18	4,6,8,9,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	7,10,16,17	4,6,8,9,15,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	7,10,14,17,18	4,6,8,9,17,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	7,10,14,16	4,6,8,9	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	7,10,14,17	4,6,8,9,15,17	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	7,10,14,16,18	4,6,8,9,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	7,10,18	4,6,8,9,13,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	7,10,16,17	4,6,8,9,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	7,10	4,6,8,9,13,15	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	7,10,16,17,18	4,6,8,9,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	7,10,14,17	4,6,8,9,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	7,10,14,16,18	4,6,8,9,13,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	7,10,14,17,18	4,6,8,9,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	7,10,14,16	4,6,8,9,13,15	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	7,10,12,17,18	4,6,8,9,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	7,10,12,16	4,6,8,9	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	7,10,12,17	4,6,8,9,15,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	7,10,12,16,18	4,6,8,9,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	7,10,12,14	4,6,8,9	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	7,10,12,14,16,17,18	4,6,8,9,17,18	2^{-1}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	7,10,12,14,18	4,6,8,9,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	7,10,12,14,16,17	4,6,8,9,15,17	2^{-1}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	7,10,12,17	4,6,8,9,13,17	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	7,10,12,16,18	4,6,8,9,13,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	7,10,12,17,18	4,6,8,9,13,15,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	7,10,12,16	4,6,8,9,13,15	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	7,10,12,14,18	4,6,8,9,13,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	7,10,12,14,16,17	4,6,8,9,13,17	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	7,10,12,14	4,6,8,9,13,15	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	7,10,12,14,16,17,18	4,6,8,9,13,15,17,18	$2^{-6.5}$

Table 0.192 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	7,10,18	4,6,8,9,11,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	7,10,16,17	4,6,8,9,11,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	7,10	4,6,8,9,11,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	7,10,16,17,18	4,6,8,9,11,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	7,10,14,17	4,6,8,9,11,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	7,10,14,16,18	4,6,8,9,11,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	7,10,14,17,18	4,6,8,9,11,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	7,10,14,16	4,6,8,9,11,15	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	7,10	4,6,8,9,11,13	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	7,10,16,17,18	4,6,8,9,11,13,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	7,10,18	4,6,8,9,11,13,15,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	7,10,16,17	4,6,8,9,11,13,15,17	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	7,10,14,17,18	4,6,8,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	7,10,14,16	4,6,8,9,11,13	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	7,10,14,17	4,6,8,9,11,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	7,10,14,16,18	4,6,8,9,11,13,15,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	7,10,12,17	4,6,8,9,11,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	7,10,12,16,18	4,6,8,9,11,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	7,10,12,17,18	4,6,8,9,11,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	7,10,12,16	4,6,8,9,11,15	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	7,10,12,14,18	4,6,8,9,11,18	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	7,10,12,14,16,17	4,6,8,9,11,17	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	7,10,12,14	4,6,8,9,11,15	$2^{-28.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	7,10,12,14,16,17,18	4,6,8,9,11,15,17,18	2^{-12}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	7,10,12,17,18	4,6,8,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	7,10,12,16	4,6,8,9,11,13	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	7,10,12,17	4,6,8,9,11,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	7,10,12,16,18	4,6,8,9,11,13,15,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	7,10,12,14	4,6,8,9,11,13	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	7,10,12,14,16,17,18	4,6,8,9,11,13,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	7,10,12,14,18	4,6,8,9,11,13,15,18	2^{-23}
$(0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	7,10,12,14,16,17	4,6,8,9,11,13,15,17	$2^{-6.5}$

Table 0.193 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	5,17	4,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	5,16,18	4,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	5,17,18	4,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	5,16	4,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	5,14,18	4,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	5,14,16,17	4,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	5,14	4,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	5,14,16,17,18	4,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	5,17,18	4,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	5,16	4,13	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	5,17	4,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	5,16,18	4,13,15,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	5,14	4,13	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	5,14,16,17,18	4,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	5,14,18	4,13,15,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	5,14,16,17	4,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	5,12,18	4,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	5,12,16,17	4,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	5,12	4,15	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	5,12,16,17,18	4,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	5,12,14,17	4,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	5,12,14,16,18	4,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	5,12,14,17,18	4,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	5,12,14,16	4,15	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	5,12	4,13	2^{-1}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	5,12,16,17,18	4,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	5,12,18	4,13,15,18	2^{-1}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	5,12,16,17	4,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	5,12,14,17,18	4,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	5,12,14,16	4,13	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	5,12,14,17	4,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	5,12,14,16,18	4,13,15,18	2^{-12}

Table 0.194 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	5,17,18	4,11,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	5,16	4,11	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	5,17	4,11,15,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	5,16,18	4,11,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	5,14	4,11	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	5,14,16,17,18	4,11,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	5,14,18	4,11,15,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	5,14,16,17	4,11,15,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	5,17	4,11,13,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	5,16,18	4,11,13,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	5,17,18	4,11,13,15,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	5,16	4,11,13,15	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	5,14,18	4,11,13,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	5,14,16,17	4,11,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	5,14	4,11,13,15	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	5,14,16,17,18	4,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	5,12	4,11	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	5,12,16,17,18	4,11,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	5,12,18	4,11,15,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	5,12,16,17	4,11,15,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	5,12,14,17,18	4,11,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	5,12,14,16	4,11	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	5,12,14,17	4,11,15,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	5,12,14,16,18	4,11,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	5,12,18	4,11,13,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	5,12,16,17	4,11,13,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	5,12	4,11,13,15	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	5,12,16,17,18	4,11,13,15,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	5,12,14,17	4,11,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	5,12,14,16,18	4,11,13,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	5,12,14,17,18	4,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	5,12,14,16	4,11,13,15	2^{-12}

Table 0.195 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	5,10,18	4,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	5,10,16,17	4,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	5,10	4,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	5,10,16,17,18	4,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	5,10,14,17	4,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	5,10,14,16,18	4,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	5,10,14,17,18	4,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	5,10,14,16	4,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	5,10	4,13	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	5,10,16,17,18	4,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	5,10,18	4,13,15,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	5,10,16,17	4,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	5,10,14,17,18	4,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	5,10,14,16	4,13	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	5,10,14,17	4,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	5,10,14,16,18	4,13,15,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	5,10,12,17	4,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	5,10,12,16,18	4,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	5,10,12,17,18	4,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	5,10,12,16	4,15	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	5,10,12,14,18	4,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	5,10,12,14,16,17	4,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	5,10,12,14	4,15	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	5,10,12,14,16,17,18	4,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	5,10,12,17,18	4,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	5,10,12,16	4,13	2^{-34}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	5,10,12,17	4,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	5,10,12,16,18	4,13,15,18	2^{-34}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	5,10,12,14	4,13	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	5,10,12,14,16,17,18	4,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	5,10,12,14,18	4,13,15,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	5,10,12,14,16,17	4,13,15,17	$2^{-17.5}$

Table 0.196 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	5,10	4,11	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	5,10,16,17,18	4,11,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	5,10,18	4,11,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	5,10,16,17	4,11,15,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	5,10,14,17,18	4,11,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	5,10,14,16	4,11	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	5,10,14,17	4,11,15,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	5,10,14,16,18	4,11,15,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	5,10,18	4,11,13,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	5,10,16,17	4,11,13,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	5,10	4,11,13,15	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	5,10,16,17,18	4,11,13,15,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	5,10,14,17	4,11,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	5,10,14,16,18	4,11,13,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	5,10,14,17,18	4,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	5,10,14,16	4,11,13,15	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	5,10,12,17,18	4,11,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	5,10,12,16	4,11	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	5,10,12,17	4,11,15,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	5,10,12,16,18	4,11,15,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	5,10,12,14	4,11	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	5,10,12,14,16,17,18	4,11,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	5,10,12,14,18	4,11,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	5,10,12,14,16,17	4,11,15,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	5,10,12,17	4,11,13,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	5,10,12,16,18	4,11,13,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	5,10,12,17,18	4,11,13,15,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	5,10,12,16	4,11,13,15	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	5,10,12,14,18	4,11,13,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	5,10,12,14,16,17	4,11,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	5,10,12,14	4,11,13,15	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	5,10,12,14,16,17,18	4,11,13,15,17,18	$2^{-17.5}$

Table 0.197 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	5,17,18	4,9,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	5,16	4,9	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	5,17	4,9,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	5,16,18	4,9,15,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	5,14	4,9	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	5,14,16,17,18	4,9,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	5,14,18	4,9,15,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	5,14,16,17	4,9,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	5,17	4,9,13,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	5,16,18	4,9,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	5,17,18	4,9,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	5,16	4,9,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	5,14,18	4,9,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	5,14,16,17	4,9,13,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	5,14	4,9,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	5,14,16,17,18	4,9,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	5,12	4,9	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	5,12,16,17,18	4,9,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	5,12,18	4,9,15,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	5,12,16,17	4,9,15,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	5,12,14,17,18	4,9,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	5,12,14,16	4,9	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	5,12,14,17	4,9,15,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	5,12,14,16,18	4,9,15,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	5,12,18	4,9,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	5,12,16,17	4,9,13,17	2^{-34}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	5,12	4,9,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	5,12,16,17,18	4,9,13,15,17,18	2^{-34}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	5,12,14,17	4,9,13,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	5,12,14,16,18	4,9,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	5,12,14,17,18	4,9,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	5,12,14,16	4,9,13,15	$2^{-17.5}$

Table 0.198 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	5,17	4,9,11,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	5,16,18	4,9,11,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	5,17,18	4,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	5,16	4,9,11,15	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	5,14,18	4,9,11,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	5,14,16,17	4,9,11,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	5,14	4,9,11,15	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	5,14,16,17,18	4,9,11,15,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	5,17,18	4,9,11,13,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	5,16	4,9,11,13	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	5,17	4,9,11,13,15,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	5,16,18	4,9,11,13,15,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	5,14	4,9,11,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	5,14,16,17,18	4,9,11,13,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	5,14,18	4,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	5,14,16,17	4,9,11,13,15,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	5,12,18	4,9,11,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	5,12,16,17	4,9,11,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	5,12	4,9,11,15	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	5,12,16,17,18	4,9,11,15,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	5,12,14,17	4,9,11,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	5,12,14,16,18	4,9,11,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	5,12,14,17,18	4,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	5,12,14,16	4,9,11,15	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	5,12	4,9,11,13	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	5,12,16,17,18	4,9,11,13,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	5,12,18	4,9,11,13,15,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	5,12,16,17	4,9,11,13,15,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	5,12,14,17,18	4,9,11,13,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	5,12,14,16	4,9,11,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	5,12,14,17	4,9,11,13,15,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	5,12,14,16,18	4,9,11,13,15,18	$2^{-17.5}$

Table 0.199 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	5,10	4,9	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	5,10,16,17,18	4,9,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	5,10,18	4,9,15,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	5,10,16,17	4,9,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	5,10,14,17,18	4,9,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	5,10,14,16	4,9	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	5,10,14,17	4,9,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	5,10,14,16,18	4,9,15,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	5,10,18	4,9,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	5,10,16,17	4,9,13,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	5,10	4,9,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	5,10,16,17,18	4,9,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	5,10,14,17	4,9,13,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	5,10,14,16,18	4,9,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	5,10,14,17,18	4,9,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	5,10,14,16	4,9,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	5,10,12,17,18	4,9,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	5,10,12,16	4,9	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	5,10,12,17	4,9,15,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	5,10,12,16,18	4,9,15,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	5,10,12,14	4,9	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	5,10,12,14,16,17,18	4,9,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	5,10,12,14,18	4,9,15,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	5,10,12,14,16,17	4,9,15,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	5,10,12,17	4,9,13,17	2^{-1}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	5,10,12,16,18	4,9,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	5,10,12,17,18	4,9,13,15,17,18	2^{-1}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	5,10,12,16	4,9,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	5,10,12,14,18	4,9,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	5,10,12,14,16,17	4,9,13,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	5,10,12,14	4,9,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	5,10,12,14,16,17,18	4,9,13,15,17,18	2^{-12}

Table 0.200 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	5,10,18	4,9,11,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	5,10,16,17	4,9,11,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	5,10	4,9,11,15	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	5,10,16,17,18	4,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	5,10,14,17	4,9,11,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	5,10,14,16,18	4,9,11,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	5,10,14,17,18	4,9,11,15,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	5,10,14,16	4,9,11,15	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	5,10	4,9,11,13	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	5,10,16,17,18	4,9,11,13,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	5,10,18	4,9,11,13,15,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	5,10,16,17	4,9,11,13,15,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	5,10,14,17,18	4,9,11,13,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	5,10,14,16	4,9,11,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	5,10,14,17	4,9,11,13,15,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	5,10,14,16,18	4,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	5,10,12,17	4,9,11,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	5,10,12,16,18	4,9,11,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	5,10,12,17,18	4,9,11,15,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	5,10,12,16	4,9,11,15	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	5,10,12,14,18	4,9,11,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	5,10,12,14,16,17	4,9,11,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	5,10,12,14	4,9,11,15	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	5,10,12,14,16,17,18	4,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	5,10,12,17,18	4,9,11,13,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	5,10,12,16	4,9,11,13	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	5,10,12,17	4,9,11,13,15,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	5,10,12,16,18	4,9,11,13,15,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	5,10,12,14	4,9,11,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	5,10,12,14,16,17,18	4,9,11,13,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	5,10,12,14,18	4,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	5,10,12,14,16,17	4,9,11,13,15,17	2^{-12}

Table 0.201 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	5,18	4,8,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	5,16,17	4,8,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	5	4,8,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	5,16,17,18	4,8,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	5,14,17	4,8,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	5,14,16,18	4,8,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	5,14,17,18	4,8,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	5,14,16	4,8,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	5	4,8,13	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	5,16,17,18	4,8,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	5,18	4,8,13,15,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	5,16,17	4,8,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	5,14,17,18	4,8,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	5,14,16	4,8,13	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	5,14,17	4,8,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	5,14,16,18	4,8,13,15,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	5,12,17	4,8,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	5,12,16,18	4,8,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	5,12,17,18	4,8,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	5,12,16	4,8,15	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	5,12,14,18	4,8,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	5,12,14,16,17	4,8,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	5,12,14	4,8,15	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	5,12,14,16,17,18	4,8,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	5,12,17,18	4,8,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	5,12,16	4,8,13	2^{-1}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	5,12,17	4,8,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	5,12,16,18	4,8,13,15,18	2^{-1}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	5,12,14	4,8,13	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	5,12,14,16,17,18	4,8,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	5,12,14,18	4,8,13,15,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	5,12,14,16,17	4,8,13,15,17	$2^{-17.5}$

Table 0.202 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	5	4,8,11	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	5,16,17,18	4,8,11,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	5,18	4,8,11,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	5,16,17	4,8,11,15,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	5,14,17,18	4,8,11,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	5,14,16	4,8,11	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	5,14,17	4,8,11,15,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	5,14,16,18	4,8,11,15,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	5,18	4,8,11,13,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	5,16,17	4,8,11,13,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	5	4,8,11,13,15	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	5,16,17,18	4,8,11,13,15,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	5,14,17	4,8,11,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	5,14,16,18	4,8,11,13,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	5,14,17,18	4,8,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	5,14,16	4,8,11,13,15	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	5,12,17,18	4,8,11,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	5,12,16	4,8,11	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	5,12,17	4,8,11,15,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	5,12,16,18	4,8,11,15,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	5,12,14	4,8,11	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	5,12,14,16,17,18	4,8,11,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	5,12,14,18	4,8,11,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	5,12,14,16,17	4,8,11,15,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	5,12,17	4,8,11,13,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	5,12,16,18	4,8,11,13,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	5,12,17,18	4,8,11,13,15,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	5,12,16	4,8,11,13,15	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	5,12,14,18	4,8,11,13,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	5,12,14,16,17	4,8,11,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	5,12,14	4,8,11,13,15	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	5,12,14,16,17,18	4,8,11,13,15,17,18	$2^{-17.5}$

Table 0.203 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	5,10,17	4,8,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	5,10,16,18	4,8,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	5,10,17,18	4,8,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	5,10,16	4,8,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	5,10,14,18	4,8,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	5,10,14,16,17	4,8,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	5,10,14	4,8,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	5,10,14,16,17,18	4,8,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	5,10,17,18	4,8,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	5,10,16	4,8,13	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	5,10,17	4,8,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	5,10,16,18	4,8,13,15,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	5,10,14	4,8,13	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	5,10,14,16,17,18	4,8,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	5,10,14,18	4,8,13,15,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	5,10,14,16,17	4,8,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	5,10,12,18	4,8,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	5,10,12,16,17	4,8,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	5,10,12	4,8,15	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	5,10,12,16,17,18	4,8,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	5,10,12,14,17	4,8,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	5,10,12,14,16,18	4,8,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	5,10,12,14,17,18	4,8,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	5,10,12,14,16	4,8,15	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	5,10,12	4,8,13	2^{-34}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	5,10,12,16,17,18	4,8,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	5,10,12,18	4,8,13,15,18	2^{-34}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	5,10,12,16,17	4,8,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	5,10,12,14,17,18	4,8,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	5,10,12,14,16	4,8,13	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	5,10,12,14,17	4,8,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	5,10,12,14,16,18	4,8,13,15,18	2^{-23}

Table 0.204 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	5,10,17,18	4,8,11,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	5,10,16	4,8,11	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	5,10,17	4,8,11,15,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	5,10,16,18	4,8,11,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	5,10,14	4,8,11	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	5,10,14,16,17,18	4,8,11,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	5,10,14,18	4,8,11,15,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	5,10,14,16,17	4,8,11,15,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	5,10,17	4,8,11,13,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	5,10,16,18	4,8,11,13,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	5,10,17,18	4,8,11,13,15,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	5,10,16	4,8,11,13,15	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	5,10,14,18	4,8,11,13,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	5,10,14,16,17	4,8,11,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	5,10,14	4,8,11,13,15	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	5,10,14,16,17,18	4,8,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	5,10,12	4,8,11	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	5,10,12,16,17,18	4,8,11,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	5,10,12,18	4,8,11,15,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	5,10,12,16,17	4,8,11,15,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	5,10,12,14,17,18	4,8,11,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	5,10,12,14,16	4,8,11	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	5,10,12,14,17	4,8,11,15,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	5,10,12,14,16,18	4,8,11,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	5,10,12,18	4,8,11,13,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	5,10,12,16,17	4,8,11,13,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	5,10,12	4,8,11,13,15	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	5,10,12,16,17,18	4,8,11,13,15,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	5,10,12,14,17	4,8,11,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	5,10,12,14,16,18	4,8,11,13,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	5,10,12,14,17,18	4,8,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	5,10,12,14,16	4,8,11,13,15	2^{-23}

Table 0.205 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	5	4,8,9	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	5,16,17,18	4,8,9,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	5,18	4,8,9,15,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	5,16,17	4,8,9,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	5,14,17,18	4,8,9,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	5,14,16	4,8,9	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	5,14,17	4,8,9,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	5,14,16,18	4,8,9,15,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	5,18	4,8,9,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	5,16,17	4,8,9,13,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	5	4,8,9,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	5,16,17,18	4,8,9,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	5,14,17	4,8,9,13,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	5,14,16,18	4,8,9,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	5,14,17,18	4,8,9,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	5,14,16	4,8,9,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	5,12,17,18	4,8,9,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	5,12,16	4,8,9	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	5,12,17	4,8,9,15,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	5,12,16,18	4,8,9,15,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	5,12,14	4,8,9	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	5,12,14,16,17,18	4,8,9,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	5,12,14,18	4,8,9,15,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	5,12,14,16,17	4,8,9,15,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	5,12,17	4,8,9,13,17	2^{-34}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	5,12,16,18	4,8,9,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	5,12,17,18	4,8,9,13,15,17,18	2^{-34}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	5,12,16	4,8,9,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	5,12,14,18	4,8,9,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	5,12,14,16,17	4,8,9,13,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	5,12,14	4,8,9,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	5,12,14,16,17,18	4,8,9,13,15,17,18	2^{-23}

Table 0.206 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	5,18	4,8,9,11,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	5,16,17	4,8,9,11,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	5	4,8,9,11,15	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	5,16,17,18	4,8,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	5,14,17	4,8,9,11,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	5,14,16,18	4,8,9,11,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	5,14,17,18	4,8,9,11,15,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	5,14,16	4,8,9,11,15	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	5	4,8,9,11,13	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	5,16,17,18	4,8,9,11,13,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	5,18	4,8,9,11,13,15,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	5,16,17	4,8,9,11,13,15,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	5,14,17,18	4,8,9,11,13,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	5,14,16	4,8,9,11,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	5,14,17	4,8,9,11,13,15,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	5,14,16,18	4,8,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	5,12,17	4,8,9,11,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	5,12,16,18	4,8,9,11,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	5,12,17,18	4,8,9,11,15,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	5,12,16	4,8,9,11,15	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	5,12,14,18	4,8,9,11,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	5,12,14,16,17	4,8,9,11,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	5,12,14	4,8,9,11,15	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	5,12,14,16,17,18	4,8,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	5,12,17,18	4,8,9,11,13,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	5,12,16	4,8,9,11,13	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	5,12,17	4,8,9,11,13,15,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	5,12,16,18	4,8,9,11,13,15,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	5,12,14	4,8,9,11,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	5,12,14,16,17,18	4,8,9,11,13,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	5,12,14,18	4,8,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	5,12,14,16,17	4,8,9,11,13,15,17	2^{-23}

Table 0.207 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	5,10,17,18	4,8,9,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	5,10,16	4,8,9	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	5,10,17	4,8,9,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	5,10,16,18	4,8,9,15,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	5,10,14	4,8,9	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	5,10,14,16,17,18	4,8,9,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	5,10,14,18	4,8,9,15,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	5,10,14,16,17	4,8,9,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	5,10,17	4,8,9,13,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	5,10,16,18	4,8,9,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	5,10,17,18	4,8,9,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	5,10,16	4,8,9,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	5,10,14,18	4,8,9,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	5,10,14,16,17	4,8,9,13,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	5,10,14	4,8,9,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	5,10,14,16,17,18	4,8,9,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	5,10,12	4,8,9	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	5,10,12,16,17,18	4,8,9,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	5,10,12,18	4,8,9,15,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	5,10,12,16,17	4,8,9,15,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	5,10,12,14,17,18	4,8,9,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	5,10,12,14,16	4,8,9	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	5,10,12,14,17	4,8,9,15,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	5,10,12,14,16,18	4,8,9,15,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	5,10,12,18	4,8,9,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	5,10,12,16,17	4,8,9,13,17	2^{-1}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	5,10,12	4,8,9,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	5,10,12,16,17,18	4,8,9,13,15,17,18	2^{-1}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	5,10,12,14,17	4,8,9,13,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	5,10,12,14,16,18	4,8,9,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	5,10,12,14,17,18	4,8,9,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	5,10,12,14,16	4,8,9,13,15	$2^{-17.5}$

Table 0.208 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,1,1,0,0,1,1,1,1,0,0,0,0,0) \xrightarrow{1r} (0,1,0,1,1,1,0,0,1,0,0,0,0,0,0,1)$	5,10,17	4,8,9,11,17	$2^{-17.5}$
$(0,0,0,1,1,0,0,1,1,1,1,0,0,0,0,1) \xrightarrow{1r} (1,0,1,0,0,0,1,1,0,1,1,1,1,1,1,1)$	5,10,16,18	4,8,9,11,18	2^{-12}
$(0,0,0,1,1,0,0,1,1,1,1,0,0,0,1,0) \xrightarrow{1r} (1,0,0,1,1,1,0,1,1,0,0,0,0,0,0,1)$	5,10,17,18	4,8,9,11,15,17,18	$2^{-17.5}$
$(0,0,0,1,1,0,0,1,1,1,1,0,0,0,1,1) \xrightarrow{1r} (0,1,1,0,0,0,1,0,0,1,1,1,1,1,1,1)$	5,10,16	4,8,9,11,15	2^{-12}
$(0,0,0,1,1,0,0,1,1,1,1,0,0,1,0,0) \xrightarrow{1r} (1,0,0,0,0,0,0,1,1,1,1,1,1,1,1,0)$	5,10,14,18	4,8,9,11,18	2^{-12}
$(0,0,0,1,1,0,0,1,1,1,1,0,0,1,0,1) \xrightarrow{1r} (0,1,1,1,1,1,0,0,0,0,0,0,0,0,0,0)$	5,10,14,16,17	4,8,9,11,17	$2^{-6.5}$
$(0,0,0,1,1,0,0,1,1,1,1,0,0,1,1,0) \xrightarrow{1r} (0,1,0,0,0,0,0,0,1,1,1,1,1,1,1,0)$	5,10,14	4,8,9,11,15	2^{-12}
$(0,0,0,1,1,0,0,1,1,1,1,0,0,1,1,1) \xrightarrow{1r} (1,0,1,1,1,1,1,1,0,0,0,0,0,0,0,0)$	5,10,14,16,17,18	4,8,9,11,15,17,18	$2^{-6.5}$
$(0,0,0,1,1,0,0,1,1,1,1,0,1,0,0,0) \xrightarrow{1r} (1,0,0,0,1,0,0,0,1,1,0,0,0,0,0,1)$	5,10,17,18	4,8,9,11,13,17,18	2^{-12}
$(0,0,0,1,1,0,0,1,1,1,1,0,1,0,0,1) \xrightarrow{1r} (0,1,1,1,0,1,1,1,0,0,1,1,1,1,1,1)$	5,10,16	4,8,9,11,13	$2^{-6.5}$
$(0,0,0,1,1,0,0,1,1,1,1,0,1,0,1,0) \xrightarrow{1r} (0,1,0,0,1,0,0,1,1,1,0,0,0,0,0,1)$	5,10,17	4,8,9,11,13,15,17	2^{-12}
$(0,0,0,1,1,0,0,1,1,1,1,0,1,0,1,1) \xrightarrow{1r} (1,0,1,1,0,1,1,0,0,0,1,1,1,1,1,1)$	5,10,16,18	4,8,9,11,13,15,18	$2^{-6.5}$
$(0,0,0,1,1,0,0,1,1,1,1,0,1,1,0,0) \xrightarrow{1r} (0,1,0,1,0,1,0,1,1,0,1,1,1,1,1,0)$	5,10,14	4,8,9,11,13	$2^{-17.5}$
$(0,0,0,1,1,0,0,1,1,1,1,0,1,1,0,1) \xrightarrow{1r} (1,0,1,0,1,0,1,0,0,1,0,0,0,0,0,0)$	5,10,14,16,17,18	4,8,9,11,13,17,18	2^{-12}
$(0,0,0,1,1,0,0,1,1,1,1,0,1,1,1,0) \xrightarrow{1r} (1,0,0,1,0,1,0,0,1,0,1,1,1,1,1,0)$	5,10,14,18	4,8,9,11,13,15,18	$2^{-17.5}$
$(0,0,0,1,1,0,0,1,1,1,1,0,1,1,1,1) \xrightarrow{1r} (0,1,1,0,1,0,1,1,0,1,0,0,0,0,0,0)$	5,10,14,16,17	4,8,9,11,13,15,17	2^{-12}
$(0,0,0,1,1,0,0,1,1,1,1,0,0,0,0,0) \xrightarrow{1r} (1,0,0,0,0,0,1,1,1,1,0,1,1,1,1,0)$	5,10,12,18	4,8,9,11,18	2^{-23}
$(0,0,0,1,1,0,0,1,1,1,1,1,0,0,0,1) \xrightarrow{1r} (0,1,1,1,1,1,0,0,0,0,1,0,0,0,0,0)$	5,10,12,16,17	4,8,9,11,17	$2^{-6.5}$
$(0,0,0,1,1,0,0,1,1,1,1,1,0,0,1,0) \xrightarrow{1r} (0,1,0,0,0,0,1,0,1,1,0,1,1,1,1,0)$	5,10,12	4,8,9,11,15	2^{-23}
$(0,0,0,1,1,0,0,1,1,1,1,1,0,0,1,1) \xrightarrow{1r} (1,0,1,1,1,1,0,1,0,0,1,0,0,0,0,0)$	5,10,12,16,17,18	4,8,9,11,15,17,18	$2^{-6.5}$
$(0,0,0,1,1,0,0,1,1,1,1,1,0,1,0,0) \xrightarrow{1r} (0,1,0,1,1,1,1,0,1,0,1,0,0,0,0,1)$	5,10,12,14,17	4,8,9,11,17	$2^{-17.5}$
$(0,0,0,1,1,0,0,1,1,1,1,1,0,1,0,1) \xrightarrow{1r} (1,0,1,0,0,0,0,1,0,1,0,1,1,1,1,1)$	5,10,12,14,16,18	4,8,9,11,18	2^{-23}
$(0,0,0,1,1,0,0,1,1,1,1,1,0,1,1,0) \xrightarrow{1r} (1,0,0,1,1,1,1,1,1,0,1,0,0,0,0,1)$	5,10,12,14,17,18	4,8,9,11,15,17,18	$2^{-17.5}$
$(0,0,0,1,1,0,0,1,1,1,1,1,0,1,1,1) \xrightarrow{1r} (0,1,1,0,0,0,0,0,0,1,0,1,1,1,1,1)$	5,10,12,14,16	4,8,9,11,15	2^{-23}
$(0,0,0,1,1,0,0,1,1,1,1,1,1,0,0,0) \xrightarrow{1r} (0,1,0,1,0,1,1,1,1,0,0,1,1,1,1,0)$	5,10,12	4,8,9,11,13	$2^{-28.5}$
$(0,0,0,1,1,0,0,1,1,1,1,1,1,0,0,1) \xrightarrow{1r} (1,0,1,0,1,0,0,0,0,1,1,0,0,0,0,0)$	5,10,12,16,17,18	4,8,9,11,13,17,18	2^{-12}
$(0,0,0,1,1,0,0,1,1,1,1,1,1,0,1,0) \xrightarrow{1r} (1,0,0,1,0,1,1,0,1,0,0,1,1,1,1,0)$	5,10,12,18	4,8,9,11,13,15,18	$2^{-28.5}$
$(0,0,0,1,1,0,0,1,1,1,1,1,1,0,1,1) \xrightarrow{1r} (0,1,1,0,1,0,0,1,0,1,1,0,0,0,0,0)$	5,10,12,16,17	4,8,9,11,13,15,17	2^{-12}
$(0,0,0,1,1,0,0,1,1,1,1,1,1,1,0,0) \xrightarrow{1r} (1,0,0,0,1,0,1,0,1,1,1,0,0,0,0,1)$	5,10,12,14,17,18	4,8,9,11,13,17,18	2^{-12}
$(0,0,0,1,1,0,0,1,1,1,1,1,1,1,0,1) \xrightarrow{1r} (0,1,1,1,0,1,0,1,0,0,0,1,1,1,1,1)$	5,10,12,14,16	4,8,9,11,13	$2^{-17.5}$
$(0,0,0,1,1,0,0,1,1,1,1,1,1,1,1,0) \xrightarrow{1r} (0,1,0,0,1,0,1,1,1,1,1,0,0,0,0,1)$	5,10,12,14,17	4,8,9,11,13,15,17	2^{-12}
$(0,0,0,1,1,0,0,1,1,1,1,1,1,1,1,1) \xrightarrow{1r} (1,0,1,1,0,1,0,0,0,0,0,1,1,1,1,1)$	5,10,12,14,16,18	4,8,9,11,13,15,18	$2^{-17.5}$

Table 0.209 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	5,7,17,18	4,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	5,7,16	4	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	5,7,17	4,15,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	5,7,16,18	4,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	5,7,14	4	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	5,7,14,16,17,18	4,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	5,7,14,18	4,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	5,7,14,16,17	4,15,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	5,7,17	4,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	5,7,16,18	4,13,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	5,7,17,18	4,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	5,7,16	4,13,15	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	5,7,14,18	4,13,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	5,7,14,16,17	4,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	5,7,14	4,13,15	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	5,7,14,16,17,18	4,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	5,7,12	4	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	5,7,12,16,17,18	4,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	5,7,12,18	4,15,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	5,7,12,16,17	4,15,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	5,7,12,14,17,18	4,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	5,7,12,14,16	4	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	5,7,12,14,17	4,15,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	5,7,12,14,16,18	4,15,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	5,7,12,18	4,13,18	2^{-1}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	5,7,12,16,17	4,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	5,7,12	4,13,15	2^{-1}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	5,7,12,16,17,18	4,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	5,7,12,14,17	4,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	5,7,12,14,16,18	4,13,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	5,7,12,14,17,18	4,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	5,7,12,14,16	4,13,15	2^{-12}

Table 0.210 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	5,7,17	4,11,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	5,7,16,18	4,11,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	5,7,17,18	4,11,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	5,7,16	4,11,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	5,7,14,18	4,11,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	5,7,14,16,17	4,11,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	5,7,14	4,11,15	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	5,7,14,16,17,18	4,11,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	5,7,17,18	4,11,13,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	5,7,16	4,11,13	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	5,7,17	4,11,13,15,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	5,7,16,18	4,11,13,15,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	5,7,14	4,11,13	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	5,7,14,16,17,18	4,11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	5,7,14,18	4,11,13,15,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	5,7,14,16,17	4,11,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	5,7,12,18	4,11,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	5,7,12,16,17	4,11,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	5,7,12	4,11,15	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	5,7,12,16,17,18	4,11,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	5,7,12,14,17	4,11,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	5,7,12,14,16,18	4,11,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	5,7,12,14,17,18	4,11,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	5,7,12,14,16	4,11,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	5,7,12	4,11,13	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	5,7,12,16,17,18	4,11,13,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	5,7,12,18	4,11,13,15,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	5,7,12,16,17	4,11,13,15,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	5,7,12,14,17,18	4,11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	5,7,12,14,16	4,11,13	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	5,7,12,14,17	4,11,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	5,7,12,14,16,18	4,11,13,15,18	2^{-12}

Table 0.211 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	5,7,10	4	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	5,7,10,16,17,18	4,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	5,7,10,18	4,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	5,7,10,16,17	4,15,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	5,7,10,14,17,18	4,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	5,7,10,14,16	4	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	5,7,10,14,17	4,15,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	5,7,10,14,16,18	4,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	5,7,10,18	4,13,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	5,7,10,16,17	4,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	5,7,10	4,13,15	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	5,7,10,16,17,18	4,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	5,7,10,14,17	4,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	5,7,10,14,16,18	4,13,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	5,7,10,14,17,18	4,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	5,7,10,14,16	4,13,15	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	5,7,10,12,17,18	4,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	5,7,10,12,16	4	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	5,7,10,12,17	4,15,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	5,7,10,12,16,18	4,15,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	5,7,10,12,14	4	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	5,7,10,12,14,16,17,18	4,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	5,7,10,12,14,18	4,15,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	5,7,10,12,14,16,17	4,15,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	5,7,10,12,17	4,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	5,7,10,12,16,18	4,13,18	2^{-34}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	5,7,10,12,17,18	4,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	5,7,10,12,16	4,13,15	2^{-34}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	5,7,10,12,14,18	4,13,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	5,7,10,12,14,16,17	4,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	5,7,10,12,14	4,13,15	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	5,7,10,12,14,16,17,18	4,13,15,17,18	$2^{-17.5}$

Table 0.212 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	5,7,10,18	4,11,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	5,7,10,16,17	4,11,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	5,7,10	4,11,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	5,7,10,16,17,18	4,11,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	5,7,10,14,17	4,11,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	5,7,10,14,16,18	4,11,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	5,7,10,14,17,18	4,11,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	5,7,10,14,16	4,11,15	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	5,7,10	4,11,13	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	5,7,10,16,17,18	4,11,13,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	5,7,10,18	4,11,13,15,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	5,7,10,16,17	4,11,13,15,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	5,7,10,14,17,18	4,11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	5,7,10,14,16	4,11,13	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	5,7,10,14,17	4,11,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	5,7,10,14,16,18	4,11,13,15,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	5,7,10,12,17	4,11,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	5,7,10,12,16,18	4,11,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	5,7,10,12,17,18	4,11,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	5,7,10,12,16	4,11,15	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	5,7,10,12,14,18	4,11,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	5,7,10,12,14,16,17	4,11,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	5,7,10,12,14	4,11,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	5,7,10,12,14,16,17,18	4,11,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	5,7,10,12,17,18	4,11,13,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	5,7,10,12,16	4,11,13	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	5,7,10,12,17	4,11,13,15,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	5,7,10,12,16,18	4,11,13,15,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	5,7,10,12,14	4,11,13	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	5,7,10,12,14,16,17,18	4,11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	5,7,10,12,14,18	4,11,13,15,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	5,7,10,12,14,16,17	4,11,13,15,17	$2^{-17.5}$

Table 0.213 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	5,7,17	4,9,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	5,7,16,18	4,9,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	5,7,17,18	4,9,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	5,7,16	4,9,15	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	5,7,14,18	4,9,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	5,7,14,16,17	4,9,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	5,7,14	4,9,15	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	5,7,14,16,17,18	4,9,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	5,7,17,18	4,9,13,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	5,7,16	4,9,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	5,7,17	4,9,13,15,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	5,7,16,18	4,9,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	5,7,14	4,9,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	5,7,14,16,17,18	4,9,13,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	5,7,14,18	4,9,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	5,7,14,16,17	4,9,13,15,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	5,7,12,18	4,9,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	5,7,12,16,17	4,9,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	5,7,12	4,9,15	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	5,7,12,16,17,18	4,9,15,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	5,7,12,14,17	4,9,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	5,7,12,14,16,18	4,9,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	5,7,12,14,17,18	4,9,15,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	5,7,12,14,16	4,9,15	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	5,7,12	4,9,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	5,7,12,16,17,18	4,9,13,17,18	2^{-34}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	5,7,12,18	4,9,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	5,7,12,16,17	4,9,13,15,17	2^{-34}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	5,7,12,14,17,18	4,9,13,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	5,7,12,14,16	4,9,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	5,7,12,14,17	4,9,13,15,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	5,7,12,14,16,18	4,9,13,15,18	$2^{-17.5}$

Table 0.214 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	5,7,17,18	4,9,11,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	5,7,16	4,9,11	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	5,7,17	4,9,11,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	5,7,16,18	4,9,11,15,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	5,7,14	4,9,11	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	5,7,14,16,17,18	4,9,11,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	5,7,14,18	4,9,11,15,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	5,7,14,16,17	4,9,11,15,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	5,7,17	4,9,11,13,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	5,7,16,18	4,9,11,13,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	5,7,17,18	4,9,11,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	5,7,16	4,9,11,13,15	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	5,7,14,18	4,9,11,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	5,7,14,16,17	4,9,11,13,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	5,7,14	4,9,11,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	5,7,14,16,17,18	4,9,11,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	5,7,12	4,9,11	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	5,7,12,16,17,18	4,9,11,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	5,7,12,18	4,9,11,15,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	5,7,12,16,17	4,9,11,15,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	5,7,12,14,17,18	4,9,11,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	5,7,12,14,16	4,9,11	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	5,7,12,14,17	4,9,11,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	5,7,12,14,16,18	4,9,11,15,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	5,7,12,18	4,9,11,13,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	5,7,12,16,17	4,9,11,13,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	5,7,12	4,9,11,13,15	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	5,7,12,16,17,18	4,9,11,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	5,7,12,14,17	4,9,11,13,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	5,7,12,14,16,18	4,9,11,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	5,7,12,14,17,18	4,9,11,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	5,7,12,14,16	4,9,11,13,15	$2^{-17.5}$

Table 0.215 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	5,7,10,18	4,9,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	5,7,10,16,17	4,9,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	5,7,10	4,9,15	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	5,7,10,16,17,18	4,9,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	5,7,10,14,17	4,9,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	5,7,10,14,16,18	4,9,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	5,7,10,14,17,18	4,9,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	5,7,10,14,16	4,9,15	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	5,7,10	4,9,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	5,7,10,16,17,18	4,9,13,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	5,7,10,18	4,9,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	5,7,10,16,17	4,9,13,15,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	5,7,10,14,17,18	4,9,13,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	5,7,10,14,16	4,9,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	5,7,10,14,17	4,9,13,15,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	5,7,10,14,16,18	4,9,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	5,7,10,12,17	4,9,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	5,7,10,12,16,18	4,9,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	5,7,10,12,17,18	4,9,15,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	5,7,10,12,16	4,9,15	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	5,7,10,12,14,18	4,9,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	5,7,10,12,14,16,17	4,9,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	5,7,10,12,14	4,9,15	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	5,7,10,12,14,16,17,18	4,9,15,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	5,7,10,12,17,18	4,9,13,17,18	2^{-1}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	5,7,10,12,16	4,9,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	5,7,10,12,17	4,9,13,15,17	2^{-1}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	5,7,10,12,16,18	4,9,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	5,7,10,12,14	4,9,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	5,7,10,12,14,16,17,18	4,9,13,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	5,7,10,12,14,18	4,9,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	5,7,10,12,14,16,17	4,9,13,15,17	2^{-12}

Table 0.216 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	5,7,10	4,9,11	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	5,7,10,16,17,18	4,9,11,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	5,7,10,18	4,9,11,15,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	5,7,10,16,17	4,9,11,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	5,7,10,14,17,18	4,9,11,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	5,7,10,14,16	4,9,11	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	5,7,10,14,17	4,9,11,15,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	5,7,10,14,16,18	4,9,11,15,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	5,7,10,18	4,9,11,13,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	5,7,10,16,17	4,9,11,13,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	5,7,10	4,9,11,13,15	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	5,7,10,16,17,18	4,9,11,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	5,7,10,14,17	4,9,11,13,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	5,7,10,14,16,18	4,9,11,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	5,7,10,14,17,18	4,9,11,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	5,7,10,14,16	4,9,11,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	5,7,10,12,17,18	4,9,11,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	5,7,10,12,16	4,9,11	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	5,7,10,12,17	4,9,11,15,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	5,7,10,12,16,18	4,9,11,15,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	5,7,10,12,14	4,9,11	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	5,7,10,12,14,16,17,18	4,9,11,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	5,7,10,12,14,18	4,9,11,15,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	5,7,10,12,14,16,17	4,9,11,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	5,7,10,12,17	4,9,11,13,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	5,7,10,12,16,18	4,9,11,13,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	5,7,10,12,17,18	4,9,11,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	5,7,10,12,16	4,9,11,13,15	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	5,7,10,12,14,18	4,9,11,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	5,7,10,12,14,16,17	4,9,11,13,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	5,7,10,12,14	4,9,11,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	5,7,10,12,14,16,17,18	4,9,11,13,15,17,18	2^{-12}

Table 0.217 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	5,7	4,8	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	5,7,16,17,18	4,8,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	5,7,18	4,8,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	5,7,16,17	4,8,15,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	5,7,14,17,18	4,8,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	5,7,14,16	4,8	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	5,7,14,17	4,8,15,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	5,7,14,16,18	4,8,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	5,7,18	4,8,13,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	5,7,16,17	4,8,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	5,7	4,8,13,15	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	5,7,16,17,18	4,8,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	5,7,14,17	4,8,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	5,7,14,16,18	4,8,13,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	5,7,14,17,18	4,8,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	5,7,14,16	4,8,13,15	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	5,7,12,17,18	4,8,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	5,7,12,16	4,8	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	5,7,12,17	4,8,15,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	5,7,12,16,18	4,8,15,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	5,7,12,14	4,8	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	5,7,12,14,16,17,18	4,8,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	5,7,12,14,18	4,8,15,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	5,7,12,14,16,17	4,8,15,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	5,7,12,17	4,8,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	5,7,12,16,18	4,8,13,18	2^{-1}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	5,7,12,17,18	4,8,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	5,7,12,16	4,8,13,15	2^{-1}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	5,7,12,14,18	4,8,13,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	5,7,12,14,16,17	4,8,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	5,7,12,14	4,8,13,15	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	5,7,12,14,16,17,18	4,8,13,15,17,18	$2^{-17.5}$

Table 0.218 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	5,7,18	4,8,11,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	5,7,16,17	4,8,11,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	5,7	4,8,11,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	5,7,16,17,18	4,8,11,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	5,7,14,17	4,8,11,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	5,7,14,16,18	4,8,11,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	5,7,14,17,18	4,8,11,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	5,7,14,16	4,8,11,15	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	5,7	4,8,11,13	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	5,7,16,17,18	4,8,11,13,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	5,7,18	4,8,11,13,15,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	5,7,16,17	4,8,11,13,15,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	5,7,14,17,18	4,8,11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	5,7,14,16	4,8,11,13	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	5,7,14,17	4,8,11,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	5,7,14,16,18	4,8,11,13,15,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	5,7,12,17	4,8,11,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	5,7,12,16,18	4,8,11,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	5,7,12,17,18	4,8,11,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	5,7,12,16	4,8,11,15	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	5,7,12,14,18	4,8,11,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	5,7,12,14,16,17	4,8,11,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	5,7,12,14	4,8,11,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	5,7,12,14,16,17,18	4,8,11,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	5,7,12,17,18	4,8,11,13,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	5,7,12,16	4,8,11,13	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	5,7,12,17	4,8,11,13,15,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	5,7,12,16,18	4,8,11,13,15,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	5,7,12,14	4,8,11,13	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	5,7,12,14,16,17,18	4,8,11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	5,7,12,14,18	4,8,11,13,15,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	5,7,12,14,16,17	4,8,11,13,15,17	$2^{-17.5}$

Table 0.219 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	5,7,10,17,18	4,8,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	5,7,10,16	4,8	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	5,7,10,17	4,8,15,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	5,7,10,16,18	4,8,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	5,7,10,14	4,8	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	5,7,10,14,16,17,18	4,8,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	5,7,10,14,18	4,8,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	5,7,10,14,16,17	4,8,15,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	5,7,10,17	4,8,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	5,7,10,16,18	4,8,13,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	5,7,10,17,18	4,8,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	5,7,10,16	4,8,13,15	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	5,7,10,14,18	4,8,13,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	5,7,10,14,16,17	4,8,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	5,7,10,14	4,8,13,15	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	5,7,10,14,16,17,18	4,8,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	5,7,10,12	4,8	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	5,7,10,12,16,17,18	4,8,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	5,7,10,12,18	4,8,15,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	5,7,10,12,16,17	4,8,15,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	5,7,10,12,14,17,18	4,8,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	5,7,10,12,14,16	4,8	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	5,7,10,12,14,17	4,8,15,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	5,7,10,12,14,16,18	4,8,15,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	5,7,10,12,18	4,8,13,18	2^{-34}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	5,7,10,12,16,17	4,8,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	5,7,10,12	4,8,13,15	2^{-34}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	5,7,10,12,16,17,18	4,8,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	5,7,10,12,14,17	4,8,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	5,7,10,12,14,16,18	4,8,13,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	5,7,10,12,14,17,18	4,8,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	5,7,10,12,14,16	4,8,13,15	2^{-23}

Table 0.220 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	5,7,10,17	4,8,11,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	5,7,10,16,18	4,8,11,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	5,7,10,17,18	4,8,11,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	5,7,10,16	4,8,11,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	5,7,10,14,18	4,8,11,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	5,7,10,14,16,17	4,8,11,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	5,7,10,14	4,8,11,15	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	5,7,10,14,16,17,18	4,8,11,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	5,7,10,17,18	4,8,11,13,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	5,7,10,16	4,8,11,13	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	5,7,10,17	4,8,11,13,15,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	5,7,10,16,18	4,8,11,13,15,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	5,7,10,14	4,8,11,13	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	5,7,10,14,16,17,18	4,8,11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	5,7,10,14,18	4,8,11,13,15,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	5,7,10,14,16,17	4,8,11,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	5,7,10,12,18	4,8,11,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	5,7,10,12,16,17	4,8,11,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	5,7,10,12	4,8,11,15	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	5,7,10,12,16,17,18	4,8,11,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	5,7,10,12,14,17	4,8,11,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	5,7,10,12,14,16,18	4,8,11,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	5,7,10,12,14,17,18	4,8,11,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	5,7,10,12,14,16	4,8,11,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	5,7,10,12	4,8,11,13	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	5,7,10,12,16,17,18	4,8,11,13,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	5,7,10,12,18	4,8,11,13,15,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	5,7,10,12,16,17	4,8,11,13,15,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	5,7,10,12,14,17,18	4,8,11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	5,7,10,12,14,16	4,8,11,13	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	5,7,10,12,14,17	4,8,11,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	5,7,10,12,14,16,18	4,8,11,13,15,18	2^{-23}

Table 0.221 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	5,7,18	4,8,9,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	5,7,16,17	4,8,9,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	5,7	4,8,9,15	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	5,7,16,17,18	4,8,9,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	5,7,14,17	4,8,9,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	5,7,14,16,18	4,8,9,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	5,7,14,17,18	4,8,9,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	5,7,14,16	4,8,9,15	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	5,7	4,8,9,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	5,7,16,17,18	4,8,9,13,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	5,7,18	4,8,9,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	5,7,16,17	4,8,9,13,15,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	5,7,14,17,18	4,8,9,13,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	5,7,14,16	4,8,9,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	5,7,14,17	4,8,9,13,15,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	5,7,14,16,18	4,8,9,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	5,7,12,17	4,8,9,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	5,7,12,16,18	4,8,9,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	5,7,12,17,18	4,8,9,15,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	5,7,12,16	4,8,9,15	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	5,7,12,14,18	4,8,9,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	5,7,12,14,16,17	4,8,9,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	5,7,12,14	4,8,9,15	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	5,7,12,14,16,17,18	4,8,9,15,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	5,7,12,17,18	4,8,9,13,17,18	2^{-34}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	5,7,12,16	4,8,9,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	5,7,12,17	4,8,9,13,15,17	2^{-34}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	5,7,12,16,18	4,8,9,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	5,7,12,14	4,8,9,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	5,7,12,14,16,17,18	4,8,9,13,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	5,7,12,14,18	4,8,9,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	5,7,12,14,16,17	4,8,9,13,15,17	2^{-23}

Table 0.222 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,1,1,0,1,1,1,0,1,0,0,0,0,0) \xrightarrow{1r} (0,1,1,0,1,0,0,1,1,1,0,1,0,0,1,0)$	5,7	4,8,9,11	2^{-23}
$(0,0,0,1,1,0,1,1,1,0,1,0,0,0,0,1) \xrightarrow{1r} (1,0,0,1,0,1,1,0,0,0,1,0,1,1,0,0)$	5,7,16,17,18	4,8,9,11,17,18	$2^{-17.5}$
$(0,0,0,1,1,0,1,1,1,0,1,0,0,0,1,0) \xrightarrow{1r} (1,0,1,0,1,0,0,0,1,1,0,1,0,0,1,0)$	5,7,18	4,8,9,11,15,18	2^{-23}
$(0,0,0,1,1,0,1,1,1,0,1,0,0,0,1,1) \xrightarrow{1r} (0,1,0,1,0,1,1,1,0,0,1,0,1,1,0,0)$	5,7,16,17	4,8,9,11,15,17	$2^{-17.5}$
$(0,0,0,1,1,0,1,1,1,0,1,0,0,1,0,0) \xrightarrow{1r} (1,0,1,1,0,1,0,0,1,0,1,0,1,1,0,1)$	5,7,14,17,18	4,8,9,11,17,18	$2^{-28.5}$
$(0,0,0,1,1,0,1,1,1,0,1,0,0,1,0,1) \xrightarrow{1r} (0,1,0,0,1,0,1,1,0,1,0,1,0,0,1,1)$	5,7,14,16	4,8,9,11	2^{-23}
$(0,0,0,1,1,0,1,1,1,0,1,0,0,1,1,0) \xrightarrow{1r} (0,1,1,1,0,1,0,1,1,0,1,0,1,1,0,1)$	5,7,14,17	4,8,9,11,15,17	$2^{-28.5}$
$(0,0,0,1,1,0,1,1,1,0,1,0,0,1,1,1) \xrightarrow{1r} (1,0,0,0,1,0,1,0,0,1,0,1,0,0,1,1)$	5,7,14,16,18	4,8,9,11,15,18	2^{-23}
$(0,0,0,1,1,0,1,1,1,0,1,0,1,0,0,0) \xrightarrow{1r} (1,0,1,1,1,0,1,1,0,1,0,0,1,0,0,1,0)$	5,7,18	4,8,9,11,13,18	$2^{-28.5}$
$(0,0,0,1,1,0,1,1,1,0,1,0,1,0,0,1) \xrightarrow{1r} (0,1,0,0,0,0,1,0,0,1,1,0,1,1,0,0)$	5,7,16,17	4,8,9,11,13,17	2^{-23}
$(0,0,0,1,1,0,1,1,1,0,1,0,1,0,1,0) \xrightarrow{1r} (0,1,1,1,1,0,0,1,0,0,1,0,0,1,0,0)$	5,7	4,8,9,11,13,15	$2^{-28.5}$
$(0,0,0,1,1,0,1,1,1,0,1,0,1,0,1,1) \xrightarrow{1r} (1,0,0,0,0,0,1,1,0,1,1,0,1,1,0,0)$	5,7,16,17,18	4,8,9,11,13,15,17,18	2^{-23}
$(0,0,0,1,1,0,1,1,1,0,1,0,1,1,0,0) \xrightarrow{1r} (0,1,1,0,0,0,0,0,1,1,1,0,1,1,0,1)$	5,7,14,17	4,8,9,11,13,17	2^{-23}
$(0,0,0,1,1,0,1,1,1,0,1,0,1,1,0,1) \xrightarrow{1r} (1,0,0,1,1,1,1,1,0,0,0,1,0,0,1,1)$	5,7,14,16,18	4,8,9,11,13,18	$2^{-17.5}$
$(0,0,0,1,1,0,1,1,1,0,1,0,1,1,1,0) \xrightarrow{1r} (1,0,1,0,0,0,0,0,1,1,1,1,0,1,1,0,1)$	5,7,14,17,18	4,8,9,11,13,15,17,18	2^{-23}
$(0,0,0,1,1,0,1,1,1,0,1,0,1,1,1,1) \xrightarrow{1r} (0,1,0,1,1,1,1,0,0,0,0,1,0,0,1,1)$	5,7,14,16	4,8,9,11,13,15	$2^{-17.5}$
$(0,0,0,1,1,0,1,1,1,0,1,1,0,0,0,0) \xrightarrow{1r} (1,0,1,1,0,1,1,0,1,0,0,0,1,1,0,1)$	5,7,12,17,18	4,8,9,11,17,18	$2^{-28.5}$
$(0,0,0,1,1,0,1,1,1,0,1,1,0,0,0,1) \xrightarrow{1r} (0,1,0,0,1,0,0,1,0,1,1,1,0,0,1,1)$	5,7,12,16	4,8,9,11	2^{-12}
$(0,0,0,1,1,0,1,1,1,0,1,1,0,0,1,0) \xrightarrow{1r} (0,1,1,1,0,1,1,1,1,0,0,0,1,1,0,1)$	5,7,12,17	4,8,9,11,15,17	$2^{-28.5}$
$(0,0,0,1,1,0,1,1,1,0,1,1,0,0,1,1) \xrightarrow{1r} (1,0,0,0,1,0,0,0,0,1,1,1,0,0,1,1)$	5,7,12,16,18	4,8,9,11,15,18	2^{-12}
$(0,0,0,1,1,0,1,1,1,0,1,1,0,1,0,0) \xrightarrow{1r} (0,1,1,0,1,0,1,1,1,1,1,1,0,0,1,0)$	5,7,12,14	4,8,9,11	2^{-12}
$(0,0,0,1,1,0,1,1,1,0,1,1,0,1,0,1) \xrightarrow{1r} (1,0,0,1,0,1,0,0,0,0,0,0,1,1,0,0)$	5,7,12,14,16,17,18	4,8,9,11,17,18	$2^{-17.5}$
$(0,0,0,1,1,0,1,1,1,0,1,1,0,1,1,0) \xrightarrow{1r} (1,0,1,0,1,0,1,0,1,1,1,1,1,0,0,1,0)$	5,7,12,14,18	4,8,9,11,15,18	2^{-12}
$(0,0,0,1,1,0,1,1,1,0,1,1,0,1,1,1) \xrightarrow{1r} (0,1,0,1,0,1,0,1,0,0,0,0,1,1,0,0)$	5,7,12,14,16,17	4,8,9,11,15,17	$2^{-17.5}$
$(0,0,0,1,1,0,1,1,1,0,1,1,1,0,0,0) \xrightarrow{1r} (0,1,1,0,0,0,1,0,1,1,0,0,1,1,0,1)$	5,7,12,17	4,8,9,11,13,17	2^{-23}
$(0,0,0,1,1,0,1,1,1,0,1,1,1,0,0,1) \xrightarrow{1r} (1,0,0,1,1,1,0,1,0,0,1,1,0,0,1,1)$	5,7,12,16,18	4,8,9,11,13,18	$2^{-6.5}$
$(0,0,0,1,1,0,1,1,1,0,1,1,1,0,1,0) \xrightarrow{1r} (1,0,1,0,0,0,1,1,1,1,0,0,1,1,0,1)$	5,7,12,17,18	4,8,9,11,13,15,17,18	2^{-23}
$(0,0,0,1,1,0,1,1,1,0,1,1,1,0,1,1) \xrightarrow{1r} (0,1,0,1,1,1,0,0,0,0,1,1,0,0,1,1)$	5,7,12,16	4,8,9,11,13,15	$2^{-6.5}$
$(0,0,0,1,1,0,1,1,1,0,1,1,1,1,0,0) \xrightarrow{1r} (1,0,1,1,1,1,1,1,1,0,1,1,0,0,1,0)$	5,7,12,14,18	4,8,9,11,13,18	$2^{-17.5}$
$(0,0,0,1,1,0,1,1,1,0,1,1,1,1,0,1) \xrightarrow{1r} (0,1,0,0,0,0,0,0,0,1,0,0,1,1,0,0)$	5,7,12,14,16,17	4,8,9,11,13,17	2^{-23}
$(0,0,0,1,1,0,1,1,1,0,1,1,1,1,1,0) \xrightarrow{1r} (0,1,1,1,1,1,1,0,1,0,1,1,0,0,1,0)$	5,7,12,14	4,8,9,11,13,15	$2^{-17.5}$
$(0,0,0,1,1,0,1,1,1,0,1,1,1,1,1,1) \xrightarrow{1r} (1,0,0,0,0,0,0,1,0,1,0,0,1,1,0,0)$	5,7,12,14,16,17,18	4,8,9,11,13,15,17,18	2^{-23}

Table 0.223 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	5,7,10,17	4,8,9,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	5,7,10,16,18	4,8,9,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	5,7,10,17,18	4,8,9,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	5,7,10,16	4,8,9,15	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	5,7,10,14,18	4,8,9,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	5,7,10,14,16,17	4,8,9,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	5,7,10,14	4,8,9,15	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	5,7,10,14,16,17,18	4,8,9,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	5,7,10,17,18	4,8,9,13,17,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	5,7,10,16	4,8,9,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	5,7,10,17	4,8,9,13,15,17	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	5,7,10,16,18	4,8,9,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	5,7,10,14	4,8,9,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	5,7,10,14,16,17,18	4,8,9,13,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	5,7,10,14,18	4,8,9,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	5,7,10,14,16,17	4,8,9,13,15,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	5,7,10,12,18	4,8,9,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	5,7,10,12,16,17	4,8,9,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	5,7,10,12	4,8,9,15	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	5,7,10,12,16,17,18	4,8,9,15,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	5,7,10,12,14,17	4,8,9,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	5,7,10,12,14,16,18	4,8,9,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	5,7,10,12,14,17,18	4,8,9,15,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	5,7,10,12,14,16	4,8,9,15	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	5,7,10,12	4,8,9,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	5,7,10,12,16,17,18	4,8,9,13,17,18	2^{-1}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	5,7,10,12,18	4,8,9,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	5,7,10,12,16,17	4,8,9,13,15,17	2^{-1}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	5,7,10,12,14,17,18	4,8,9,13,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	5,7,10,12,14,16	4,8,9,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	5,7,10,12,14,17	4,8,9,13,15,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	5,7,10,12,14,16,18	4,8,9,13,15,18	$2^{-17.5}$

Table 0.224 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	5,7,10,17,18	4,8,9,11,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	5,7,10,16	4,8,9,11	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	5,7,10,17	4,8,9,11,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	5,7,10,16,18	4,8,9,11,15,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	5,7,10,14	4,8,9,11	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	5,7,10,14,16,17,18	4,8,9,11,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	5,7,10,14,18	4,8,9,11,15,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	5,7,10,14,16,17	4,8,9,11,15,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	5,7,10,17	4,8,9,11,13,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	5,7,10,16,18	4,8,9,11,13,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	5,7,10,17,18	4,8,9,11,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	5,7,10,16	4,8,9,11,13,15	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	5,7,10,14,18	4,8,9,11,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	5,7,10,14,16,17	4,8,9,11,13,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	5,7,10,14	4,8,9,11,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	5,7,10,14,16,17,18	4,8,9,11,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	5,7,10,12	4,8,9,11	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	5,7,10,12,16,17,18	4,8,9,11,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	5,7,10,12,18	4,8,9,11,15,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	5,7,10,12,16,17	4,8,9,11,15,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	5,7,10,12,14,17,18	4,8,9,11,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	5,7,10,12,14,16	4,8,9,11	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	5,7,10,12,14,17	4,8,9,11,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	5,7,10,12,14,16,18	4,8,9,11,15,18	2^{-23}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	5,7,10,12,18	4,8,9,11,13,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	5,7,10,12,16,17	4,8,9,11,13,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	5,7,10,12	4,8,9,11,13,15	$2^{-28.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	5,7,10,12,16,17,18	4,8,9,11,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	5,7,10,12,14,17	4,8,9,11,13,17	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	5,7,10,12,14,16,18	4,8,9,11,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	5,7,10,12,14,17,18	4,8,9,11,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	5,7,10,12,14,16	4,8,9,11,13,15	$2^{-17.5}$

Table 0.225 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	5,18	4,6,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	5,16,17	4,6,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	5	4,6,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	5,16,17,18	4,6,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	5,14,17	4,6,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	5,14,16,18	4,6,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	5,14,17,18	4,6,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	5,14,16	4,6,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	5	4,6,13	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	5,16,17,18	4,6,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	5,18	4,6,13,15,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	5,16,17	4,6,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	5,14,17,18	4,6,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	5,14,16	4,6,13	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	5,14,17	4,6,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	5,14,16,18	4,6,13,15,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	5,12,17	4,6,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	5,12,16,18	4,6,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	5,12,17,18	4,6,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	5,12,16	4,6,15	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	5,12,14,18	4,6,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	5,12,14,16,17	4,6,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	5,12,14	4,6,15	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	5,12,14,16,17,18	4,6,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	5,12,17,18	4,6,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	5,12,16	4,6,13	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	5,12,17	4,6,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	5,12,16,18	4,6,13,15,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	5,12,14	4,6,13	2^{-1}
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	5,12,14,16,17,18	4,6,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	5,12,14,18	4,6,13,15,18	2^{-1}
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	5,12,14,16,17	4,6,13,15,17	$2^{-17.5}$

Table 0.226 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	5	4,6,11	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	5,16,17,18	4,6,11,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	5,18	4,6,11,15,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	5,16,17	4,6,11,15,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	5,14,17,18	4,6,11,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	5,14,16	4,6,11	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	5,14,17	4,6,11,15,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	5,14,16,18	4,6,11,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	5,18	4,6,11,13,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	5,16,17	4,6,11,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	5	4,6,11,13,15	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	5,16,17,18	4,6,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	5,14,17	4,6,11,13,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	5,14,16,18	4,6,11,13,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	5,14,17,18	4,6,11,13,15,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	5,14,16	4,6,11,13,15	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	5,12,17,18	4,6,11,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	5,12,16	4,6,11	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	5,12,17	4,6,11,15,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	5,12,16,18	4,6,11,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	5,12,14	4,6,11	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	5,12,14,16,17,18	4,6,11,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	5,12,14,18	4,6,11,15,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	5,12,14,16,17	4,6,11,15,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	5,12,17	4,6,11,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	5,12,16,18	4,6,11,13,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	5,12,17,18	4,6,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	5,12,16	4,6,11,13,15	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	5,12,14,18	4,6,11,13,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	5,12,14,16,17	4,6,11,13,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	5,12,14	4,6,11,13,15	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	5,12,14,16,17,18	4,6,11,13,15,17,18	$2^{-28.5}$

Table 0.227 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,1,1,1,0,0,0,1,0,0,0,0,0,0) \xrightarrow{1r} (0,0,1,0,1,1,0,1,0,0,0,0,1,1,1,1)$	5,10,17	4,6,17	2^{-12}
$(0,0,0,1,1,1,0,0,0,1,0,0,0,0,0,1) \xrightarrow{1r} (1,1,0,1,0,0,1,0,1,1,1,1,0,0,0,1)$	5,10,16,18	4,6,18	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,0,1,0,0,0,0,1,0) \xrightarrow{1r} (1,1,1,0,1,1,0,0,0,0,0,0,1,1,1,1)$	5,10,17,18	4,6,15,17,18	2^{-12}
$(0,0,0,1,1,1,0,0,0,1,0,0,0,0,1,1) \xrightarrow{1r} (0,0,0,1,0,0,1,1,1,1,1,1,0,0,0,1)$	5,10,16	4,6,15	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,0,1,0,0,0,1,0,0) \xrightarrow{1r} (1,1,1,1,0,0,0,0,0,1,1,1,0,0,0,0)$	5,10,14,18	4,6,18	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,0,1,0,0,0,1,0,1) \xrightarrow{1r} (0,0,0,0,1,1,1,1,1,0,0,0,1,1,1,0)$	5,10,14,16,17	4,6,17	2^{-23}
$(0,0,0,1,1,1,0,0,0,1,0,0,0,1,1,0) \xrightarrow{1r} (0,0,1,1,0,0,0,1,0,1,1,1,0,0,0,0)$	5,10,14	4,6,15	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,0,1,0,0,0,1,1,1) \xrightarrow{1r} (1,1,0,0,1,1,1,0,1,0,0,0,1,1,1,0)$	5,10,14,16,17,18	4,6,15,17,18	2^{-23}
$(0,0,0,1,1,1,0,0,0,1,0,0,1,0,0,0) \xrightarrow{1r} (1,1,1,1,1,0,0,1,0,1,0,0,1,1,1,1)$	5,10,17,18	4,6,13,17,18	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,0,1,0,0,1,0,0,1) \xrightarrow{1r} (0,0,0,0,0,1,1,0,1,0,1,0,1,0,0,0,1)$	5,10,16	4,6,13	2^{-23}
$(0,0,0,1,1,1,0,0,0,1,0,0,1,0,1,0) \xrightarrow{1r} (0,0,1,1,1,0,0,0,0,1,0,0,1,1,1,1)$	5,10,17	4,6,13,15,17	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,0,1,0,0,1,0,1,1) \xrightarrow{1r} (1,1,0,0,0,1,1,1,1,0,1,1,0,0,0,0,1)$	5,10,16,18	4,6,13,15,18	2^{-23}
$(0,0,0,1,1,1,0,0,0,1,0,0,1,1,0,0) \xrightarrow{1r} (0,0,1,0,0,1,0,0,0,0,1,1,0,0,0,0)$	5,10,14	4,6,13	2^{-12}
$(0,0,0,1,1,1,0,0,0,1,0,0,1,1,0,1) \xrightarrow{1r} (1,1,0,1,1,0,1,1,1,1,0,0,1,1,1,0)$	5,10,14,16,17,18	4,6,13,17,18	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,0,1,0,0,1,1,1,0) \xrightarrow{1r} (1,1,1,0,0,1,0,1,0,0,1,1,0,0,0,0)$	5,10,14,18	4,6,13,15,18	2^{-12}
$(0,0,0,1,1,1,0,0,0,1,0,0,1,1,1,1) \xrightarrow{1r} (0,0,0,1,1,0,1,0,1,1,0,0,1,1,1,0)$	5,10,14,16,17	4,6,13,15,17	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,0,1,0,1,0,0,0,0) \xrightarrow{1r} (1,1,1,1,0,0,1,0,0,1,0,1,0,0,0,0)$	5,10,12,18	4,6,18	$2^{-28.5}$
$(0,0,0,1,1,1,0,0,0,1,0,1,0,0,0,1) \xrightarrow{1r} (0,0,0,0,1,1,0,1,1,0,1,0,1,1,1,0)$	5,10,12,16,17	4,6,17	2^{-23}
$(0,0,0,1,1,1,0,0,0,1,0,1,0,0,1,0) \xrightarrow{1r} (0,0,1,1,0,0,1,1,0,1,0,1,0,0,0,0)$	5,10,12	4,6,15	$2^{-28.5}$
$(0,0,0,1,1,1,0,0,0,1,0,1,0,0,1,1) \xrightarrow{1r} (1,1,0,0,1,1,0,0,1,0,1,0,1,1,1,0)$	5,10,12,16,17,18	4,6,15,17,18	2^{-23}
$(0,0,0,1,1,1,0,0,0,1,0,1,0,1,0,0) \xrightarrow{1r} (0,0,1,0,1,1,1,1,0,0,1,0,1,1,1,1)$	5,10,12,14,17	4,6,17	2^{-12}
$(0,0,0,1,1,1,0,0,0,1,0,1,0,1,0,1) \xrightarrow{1r} (1,1,0,1,0,0,0,0,1,1,0,1,0,0,0,1)$	5,10,12,14,16,18	4,6,18	$2^{-28.5}$
$(0,0,0,1,1,1,0,0,0,1,0,1,0,1,1,0) \xrightarrow{1r} (1,1,1,0,1,1,1,0,0,0,1,0,1,1,1,1)$	5,10,12,14,17,18	4,6,15,17,18	2^{-12}
$(0,0,0,1,1,1,0,0,0,1,0,1,0,1,1,1) \xrightarrow{1r} (0,0,0,1,0,0,0,1,1,1,0,1,0,0,0,1)$	5,10,12,14,16	4,6,15	$2^{-28.5}$
$(0,0,0,1,1,1,0,0,0,1,0,1,1,0,0,0) \xrightarrow{1r} (0,0,1,0,0,1,1,0,0,0,0,1,0,0,0,0)$	5,10,12	4,6,13	2^{-23}
$(0,0,0,1,1,1,0,0,0,1,0,1,1,0,0,1) \xrightarrow{1r} (1,1,0,1,1,0,0,1,1,1,1,0,1,1,1,0)$	5,10,12,16,17,18	4,6,13,17,18	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,0,1,0,1,1,0,1,0) \xrightarrow{1r} (1,1,1,0,0,1,1,1,0,0,0,1,0,0,0,0)$	5,10,12,18	4,6,13,15,18	2^{-23}
$(0,0,0,1,1,1,0,0,0,1,0,1,1,0,1,1) \xrightarrow{1r} (0,0,0,1,1,0,0,0,1,1,1,0,1,1,1,0)$	5,10,12,16,17	4,6,13,15,17	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,0,1,0,1,1,1,0,0) \xrightarrow{1r} (1,1,1,1,1,0,1,1,0,1,1,0,1,1,1,1)$	5,10,12,14,17,18	4,6,13,17,18	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,0,1,0,1,1,1,0,1) \xrightarrow{1r} (0,0,0,0,0,1,0,0,1,0,0,1,0,0,0,1)$	5,10,12,14,16	4,6,13	2^{-34}
$(0,0,0,1,1,1,0,0,0,1,0,1,1,1,1,0) \xrightarrow{1r} (0,0,1,1,1,0,1,0,0,1,1,0,1,1,1,1)$	5,10,12,14,17	4,6,13,15,17	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,0,1,0,1,1,1,1,1) \xrightarrow{1r} (1,1,0,0,0,1,0,1,1,0,0,1,0,0,0,1)$	5,10,12,14,16,18	4,6,13,15,18	2^{-34}

Table 0.228 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,1,1,1,0,0,0,1,1,0,0,0,0,0) \xrightarrow{1r} (1,1,1,0,1,0,0,1,0,1,0,1,1,1,1,1)$	5,10,17,18	4,6,11,17,18	2^{-23}
$(0,0,0,1,1,1,0,0,0,1,1,0,0,0,0,1) \xrightarrow{1r} (0,0,0,1,0,1,1,0,1,0,1,0,0,0,0,1)$	5,10,16	4,6,11	$2^{-28.5}$
$(0,0,0,1,1,1,0,0,0,1,1,0,0,0,1,0) \xrightarrow{1r} (0,0,1,0,1,0,0,0,0,1,0,1,1,1,1,1)$	5,10,17	4,6,11,15,17	2^{-23}
$(0,0,0,1,1,1,0,0,0,1,1,0,0,0,1,1) \xrightarrow{1r} (1,1,0,1,0,1,1,1,1,0,1,0,0,0,0,1)$	5,10,16,18	4,6,11,15,18	$2^{-28.5}$
$(0,0,0,1,1,1,0,0,0,1,1,0,0,1,0,0) \xrightarrow{1r} (0,0,1,1,0,1,0,0,0,0,1,0,0,0,0,0)$	5,10,14	4,6,11	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,0,1,1,0,0,1,0,1) \xrightarrow{1r} (1,1,0,0,1,0,1,1,1,1,0,1,1,1,1,0)$	5,10,14,16,17,18	4,6,11,17,18	2^{-23}
$(0,0,0,1,1,1,0,0,0,1,1,0,0,1,1,0) \xrightarrow{1r} (1,1,1,1,0,1,0,1,0,0,1,0,0,0,0,0)$	5,10,14,18	4,6,11,15,18	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,0,1,1,0,0,1,1,1) \xrightarrow{1r} (0,0,0,0,1,0,1,0,1,1,0,1,1,1,1,0)$	5,10,14,16,17	4,6,11,15,17	2^{-23}
$(0,0,0,1,1,1,0,0,0,1,1,0,1,0,0,0) \xrightarrow{1r} (0,0,1,1,1,1,0,1,0,0,0,1,1,1,1,1)$	5,10,17	4,6,11,13,17	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,0,1,1,0,1,0,0,1) \xrightarrow{1r} (1,1,0,0,0,0,1,0,1,1,1,0,0,0,0,1)$	5,10,16,18	4,6,11,13,18	2^{-23}
$(0,0,0,1,1,1,0,0,0,1,1,0,1,0,1,0) \xrightarrow{1r} (1,1,1,1,1,1,0,0,0,0,0,1,1,1,1,1)$	5,10,17,18	4,6,11,13,15,17,18	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,0,1,1,0,1,0,1,1) \xrightarrow{1r} (0,0,0,0,0,0,1,1,1,1,1,0,0,0,0,1)$	5,10,16	4,6,11,13,15	2^{-23}
$(0,0,0,1,1,1,0,0,0,1,1,0,1,1,0,0) \xrightarrow{1r} (1,1,1,0,0,0,0,0,0,1,1,0,0,0,0,0)$	5,10,14,18	4,6,11,13,18	2^{-23}
$(0,0,0,1,1,1,0,0,0,1,1,0,1,1,0,1) \xrightarrow{1r} (0,0,0,1,1,1,1,1,0,0,1,1,1,1,0,0)$	5,10,14,16,17	4,6,11,13,17	$2^{-28.5}$
$(0,0,0,1,1,1,0,0,0,1,1,0,1,1,1,0) \xrightarrow{1r} (0,0,1,0,0,0,0,1,0,1,1,0,0,0,0,0)$	5,10,14	4,6,11,13,15	2^{-23}
$(0,0,0,1,1,1,0,0,0,1,1,0,1,1,1,1) \xrightarrow{1r} (1,1,0,1,1,1,1,0,1,0,0,1,1,1,1,0)$	5,10,14,16,17,18	4,6,11,13,15,17,18	$2^{-28.5}$
$(0,0,0,1,1,1,0,0,0,1,1,1,0,0,0,0) \xrightarrow{1r} (0,0,1,1,0,1,1,0,0,0,0,0,0,0,0,0)$	5,10,12	4,6,11	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,0,1,1,1,0,0,0,1) \xrightarrow{1r} (1,1,0,0,1,0,0,1,1,1,1,1,1,1,1,0)$	5,10,12,16,17,18	4,6,11,17,18	2^{-12}
$(0,0,0,1,1,1,0,0,0,1,1,1,0,0,1,0) \xrightarrow{1r} (1,1,1,1,0,1,1,1,0,0,0,0,0,0,0,0)$	5,10,12,18	4,6,11,15,18	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,0,1,1,1,0,0,1,1) \xrightarrow{1r} (0,0,0,0,1,0,0,0,1,1,1,1,1,1,1,0)$	5,10,12,16,17	4,6,11,15,17	2^{-12}
$(0,0,0,1,1,1,0,0,0,1,1,1,0,1,0,0) \xrightarrow{1r} (1,1,1,0,1,0,1,1,0,1,1,1,1,1,1,1)$	5,10,12,14,17,18	4,6,11,17,18	2^{-12}
$(0,0,0,1,1,1,0,0,0,1,1,1,0,1,0,1) \xrightarrow{1r} (0,0,0,1,0,1,0,0,1,0,0,0,0,0,0,1)$	5,10,12,14,16	4,6,11	$2^{-28.5}$
$(0,0,0,1,1,1,0,0,0,1,1,1,0,1,1,0) \xrightarrow{1r} (0,0,1,0,1,0,1,0,0,1,1,1,1,1,1,1)$	5,10,12,14,17	4,6,11,15,17	2^{-12}
$(0,0,0,1,1,1,0,0,0,1,1,1,0,1,1,1) \xrightarrow{1r} (1,1,0,1,0,1,0,1,1,0,0,0,0,0,0,1)$	5,10,12,14,16,18	4,6,11,15,18	$2^{-28.5}$
$(0,0,0,1,1,1,0,0,0,1,1,1,1,0,0,0) \xrightarrow{1r} (1,1,1,0,0,0,1,0,0,1,0,0,0,0,0,0)$	5,10,12,18	4,6,11,13,18	2^{-23}
$(0,0,0,1,1,1,0,0,0,1,1,1,1,0,0,1) \xrightarrow{1r} (0,0,0,1,1,1,0,1,1,0,1,1,1,1,1,0)$	5,10,12,16,17	4,6,11,13,17	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,0,1,1,1,1,0,1,0) \xrightarrow{1r} (0,0,1,0,0,0,1,1,0,1,0,0,0,0,0,0)$	5,10,12	4,6,11,13,15	2^{-23}
$(0,0,0,1,1,1,0,0,0,1,1,1,1,0,1,1) \xrightarrow{1r} (1,1,0,1,1,1,0,0,1,0,1,1,1,1,1,0)$	5,10,12,16,17,18	4,6,11,13,15,17,18	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,0,1,1,1,1,1,0,0) \xrightarrow{1r} (0,0,1,1,1,1,1,1,0,0,1,1,1,1,1,1)$	5,10,12,14,17	4,6,11,13,17	$2^{-6.5}$
$(0,0,0,1,1,1,0,0,0,1,1,1,1,1,0,1) \xrightarrow{1r} (1,1,0,0,0,0,0,0,1,1,0,0,0,0,0,1)$	5,10,12,14,16,18	4,6,11,13,18	2^{-23}
$(0,0,0,1,1,1,0,0,0,1,1,1,1,1,1,0) \xrightarrow{1r} (1,1,1,1,1,1,1,0,0,0,1,1,1,1,1,1)$	5,10,12,14,17,18	4,6,11,13,15,17,18	$2^{-6.5}$
$(0,0,0,1,1,1,0,0,0,1,1,1,1,1,1,1) \xrightarrow{1r} (0,0,0,0,0,0,0,1,1,1,0,0,0,0,0,1)$	5,10,12,14,16	4,6,11,13,15	2^{-23}

Table 0.229 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	5	4,6,9	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	5,16,17,18	4,6,9,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	5,18	4,6,9,15,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	5,16,17	4,6,9,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	5,14,17,18	4,6,9,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	5,14,16	4,6,9	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	5,14,17	4,6,9,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	5,14,16,18	4,6,9,15,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	5,18	4,6,9,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	5,16,17	4,6,9,13,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	5	4,6,9,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	5,16,17,18	4,6,9,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	5,14,17	4,6,9,13,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	5,14,16,18	4,6,9,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	5,14,17,18	4,6,9,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	5,14,16	4,6,9,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	5,12,17,18	4,6,9,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	5,12,16	4,6,9	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	5,12,17	4,6,9,15,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	5,12,16,18	4,6,9,15,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	5,12,14	4,6,9	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	5,12,14,16,17,18	4,6,9,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	5,12,14,18	4,6,9,15,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	5,12,14,16,17	4,6,9,15,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	5,12,17	4,6,9,13,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	5,12,16,18	4,6,9,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	5,12,17,18	4,6,9,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	5,12,16	4,6,9,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	5,12,14,18	4,6,9,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	5,12,14,16,17	4,6,9,13,17	2^{-34}
$(0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	5,12,14	4,6,9,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	5,12,14,16,17,18	4,6,9,13,15,17,18	2^{-34}

Table 0.230 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,1,1,1,0,0,1,0,1,0,0,0,0,0) \xrightarrow{1r} (1,0,0,0,1,0,0,1,0,1,0,1,1,1,0,0)$	5,18	4,6,9,11,18	2^{-23}
$(0,0,0,1,1,1,0,0,1,0,1,0,0,0,0,1) \xrightarrow{1r} (0,1,1,1,0,1,1,0,1,0,1,0,0,0,1,0)$	5,16,17	4,6,9,11,17	$2^{-28.5}$
$(0,0,0,1,1,1,0,0,1,0,1,0,0,0,1,0) \xrightarrow{1r} (0,1,0,0,1,0,0,0,0,1,0,1,1,1,0,0)$	5	4,6,9,11,15	2^{-23}
$(0,0,0,1,1,1,0,0,1,0,1,0,0,0,1,1) \xrightarrow{1r} (1,0,1,1,0,1,1,1,1,0,1,0,0,0,1,0)$	5,16,17,18	4,6,9,11,15,17,18	$2^{-28.5}$
$(0,0,0,1,1,1,0,0,1,0,1,0,0,1,0,0) \xrightarrow{1r} (0,1,0,1,0,1,0,0,0,0,1,0,0,0,1,1)$	5,14,17	4,6,9,11,17	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,1,0,1,0,0,1,0,1) \xrightarrow{1r} (1,0,1,0,1,0,1,1,1,1,0,1,1,1,0,1)$	5,14,16,18	4,6,9,11,18	2^{-23}
$(0,0,0,1,1,1,0,0,1,0,1,0,0,1,1,0) \xrightarrow{1r} (1,0,0,1,0,1,0,1,0,0,1,0,0,0,1,1)$	5,14,17,18	4,6,9,11,15,17,18	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,1,0,1,0,0,1,1,1) \xrightarrow{1r} (0,1,1,0,1,0,1,0,1,1,0,1,1,1,0,1)$	5,14,16	4,6,9,11,15	2^{-23}
$(0,0,0,1,1,1,0,0,1,0,1,0,1,0,0,0) \xrightarrow{1r} (0,1,0,1,1,1,0,1,0,0,0,1,1,1,0,0)$	5	4,6,9,11,13	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,1,0,1,0,1,0,0,1) \xrightarrow{1r} (1,0,1,0,0,0,1,0,1,1,1,0,0,0,1,0)$	5,16,17,18	4,6,9,11,13,17,18	2^{-23}
$(0,0,0,1,1,1,0,0,1,0,1,0,1,0,1,0) \xrightarrow{1r} (1,0,0,1,1,1,0,0,0,0,0,1,1,1,0,0)$	5,18	4,6,9,11,13,15,18	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,1,0,1,0,1,0,1,1) \xrightarrow{1r} (0,1,1,0,0,0,1,1,1,1,1,0,0,0,1,0)$	5,16,17	4,6,9,11,13,15,17	2^{-23}
$(0,0,0,1,1,1,0,0,1,0,1,0,1,1,0,0) \xrightarrow{1r} (1,0,0,0,0,0,0,0,0,0,1,1,0,0,0,1,1)$	5,14,17,18	4,6,9,11,13,17,18	2^{-23}
$(0,0,0,1,1,1,0,0,1,0,1,0,1,1,0,1) \xrightarrow{1r} (0,1,1,1,1,1,1,1,0,0,1,1,1,0,1,1)$	5,14,16	4,6,9,11,13	$2^{-28.5}$
$(0,0,0,1,1,1,0,0,1,0,1,0,1,1,1,0) \xrightarrow{1r} (0,1,0,0,0,0,0,1,0,1,1,0,0,0,1,1)$	5,14,17	4,6,9,11,13,15,17	2^{-23}
$(0,0,0,1,1,1,0,0,1,0,1,0,1,1,1,1) \xrightarrow{1r} (1,0,1,1,1,1,1,0,1,0,0,1,1,1,0,1)$	5,14,16,18	4,6,9,11,13,15,18	$2^{-28.5}$
$(0,0,0,1,1,1,0,0,1,0,1,1,0,0,0,0) \xrightarrow{1r} (0,1,0,1,0,1,1,0,0,0,0,0,0,0,1,1)$	5,12,17	4,6,9,11,17	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,1,0,1,1,0,0,0,1) \xrightarrow{1r} (1,0,1,0,1,0,0,1,1,1,1,1,1,1,0,1)$	5,12,16,18	4,6,9,11,18	2^{-12}
$(0,0,0,1,1,1,0,0,1,0,1,1,0,0,1,0) \xrightarrow{1r} (1,0,0,1,0,1,1,1,0,0,0,0,0,0,1,1)$	5,12,17,18	4,6,9,11,15,17,18	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,1,0,1,1,0,0,1,1) \xrightarrow{1r} (0,1,1,0,1,0,0,0,1,1,1,1,1,1,0,1)$	5,12,16	4,6,9,11,15	2^{-12}
$(0,0,0,1,1,1,0,0,1,0,1,1,0,1,0,0) \xrightarrow{1r} (1,0,0,0,1,0,1,1,0,1,1,1,1,1,0,0)$	5,12,14,18	4,6,9,11,18	2^{-12}
$(0,0,0,1,1,1,0,0,1,0,1,1,0,1,0,1) \xrightarrow{1r} (0,1,1,1,0,1,0,0,1,0,0,0,0,0,1,0)$	5,12,14,16,17	4,6,9,11,17	$2^{-28.5}$
$(0,0,0,1,1,1,0,0,1,0,1,1,0,1,1,0) \xrightarrow{1r} (0,1,0,0,1,0,1,0,0,1,1,1,1,1,0,0)$	5,12,14	4,6,9,11,15	2^{-12}
$(0,0,0,1,1,1,0,0,1,0,1,1,0,1,1,1) \xrightarrow{1r} (1,0,1,1,0,1,0,1,1,0,0,0,0,0,1,0)$	5,12,14,16,17,18	4,6,9,11,15,17,18	$2^{-28.5}$
$(0,0,0,1,1,1,0,0,1,0,1,1,1,0,0,0) \xrightarrow{1r} (1,0,0,0,0,0,1,0,0,1,0,0,0,0,1,1)$	5,12,17,18	4,6,9,11,13,17,18	2^{-23}
$(0,0,0,1,1,1,0,0,1,0,1,1,1,0,0,1) \xrightarrow{1r} (0,1,1,1,1,1,0,1,1,0,1,1,1,1,0,1)$	5,12,16	4,6,9,11,13	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,1,0,1,1,1,0,1,0) \xrightarrow{1r} (0,1,0,0,0,0,1,1,0,1,0,0,0,0,1,1)$	5,12,17	4,6,9,11,13,15,17	2^{-23}
$(0,0,0,1,1,1,0,0,1,0,1,1,1,0,1,1) \xrightarrow{1r} (1,0,1,1,1,1,0,0,1,0,1,1,1,1,0,1)$	5,12,16,18	4,6,9,11,13,15,18	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,1,0,1,1,1,1,0,0) \xrightarrow{1r} (0,1,0,1,1,1,1,1,0,0,1,1,1,1,0,0)$	5,12,14	4,6,9,11,13	$2^{-6.5}$
$(0,0,0,1,1,1,0,0,1,0,1,1,1,1,0,1) \xrightarrow{1r} (1,0,1,0,0,0,0,0,1,1,0,0,0,0,1,0)$	5,12,14,16,17,18	4,6,9,11,13,17,18	2^{-23}
$(0,0,0,1,1,1,0,0,1,0,1,1,1,1,1,0) \xrightarrow{1r} (1,0,0,1,1,1,1,0,0,0,1,1,1,1,0,0)$	5,12,14,18	4,6,9,11,13,15,18	$2^{-6.5}$
$(0,0,0,1,1,1,0,0,1,0,1,1,1,1,1,1) \xrightarrow{1r} (0,1,1,0,0,0,0,1,1,1,0,0,0,0,1,0)$	5,12,14,16,17	4,6,9,11,13,15,17	2^{-23}

Table 0.231 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,1,1,1,0,0,1,1,0,0,0,0,0,0) \xrightarrow{1r} (1,0,1,1,1,0,0,0,0,1,0,1,1,0,1,1)$	5,10,17,18	4,6,9,17,18	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,1,1,0,0,0,0,0,1) \xrightarrow{1r} (0,1,0,0,0,1,1,1,1,0,1,0,0,1,0,1)$	5,10,16	4,6,9	2^{-23}
$(0,0,0,1,1,1,0,0,1,1,0,0,0,0,1,0) \xrightarrow{1r} (0,1,1,1,1,0,0,1,0,1,0,1,1,0,1,1)$	5,10,17	4,6,9,15,17	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,1,1,0,0,0,0,1,1) \xrightarrow{1r} (1,0,0,0,0,1,1,0,1,0,1,0,0,1,0,1)$	5,10,16,18	4,6,9,15,18	2^{-23}
$(0,0,0,1,1,1,0,0,1,1,0,0,0,1,0,0) \xrightarrow{1r} (0,1,1,0,0,1,0,1,0,0,1,0,0,1,0,0)$	5,10,14	4,6,9	2^{-12}
$(0,0,0,1,1,1,0,0,1,1,0,0,0,1,0,1) \xrightarrow{1r} (1,0,0,1,1,0,1,0,1,1,0,1,1,0,1,0)$	5,10,14,16,17,18	4,6,9,17,18	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,1,1,0,0,0,1,1,0) \xrightarrow{1r} (1,0,1,0,0,1,0,0,0,0,1,0,0,1,0,0)$	5,10,14,18	4,6,9,15,18	2^{-12}
$(0,0,0,1,1,1,0,0,1,1,0,0,0,1,1,1) \xrightarrow{1r} (0,1,0,1,1,0,1,1,1,1,0,1,1,0,1,0)$	5,10,14,16,17	4,6,9,15,17	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,1,1,0,0,1,0,0,0) \xrightarrow{1r} (0,1,1,0,1,1,0,0,0,0,0,1,1,0,1,1)$	5,10,17	4,6,9,13,17	2^{-12}
$(0,0,0,1,1,1,0,0,1,1,0,0,1,0,0,1) \xrightarrow{1r} (1,0,0,1,0,0,1,1,1,1,1,0,0,1,0,1)$	5,10,16,18	4,6,9,13,18	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,1,1,0,0,1,0,1,0) \xrightarrow{1r} (1,0,1,0,1,1,0,1,0,0,0,1,1,0,1,1)$	5,10,17,18	4,6,9,13,15,17,18	2^{-12}
$(0,0,0,1,1,1,0,0,1,1,0,0,1,0,1,1) \xrightarrow{1r} (0,1,0,1,0,0,1,0,1,1,1,0,0,1,0,1)$	5,10,16	4,6,9,13,15	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,1,1,0,0,1,1,0,0) \xrightarrow{1r} (1,0,1,1,0,0,0,1,0,1,1,0,0,1,0,0)$	5,10,14,18	4,6,9,13,18	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,1,1,0,0,1,1,0,1) \xrightarrow{1r} (0,1,0,0,1,1,1,0,1,0,0,1,1,0,1,0)$	5,10,14,16,17	4,6,9,13,17	2^{-23}
$(0,0,0,1,1,1,0,0,1,1,0,0,1,1,1,0) \xrightarrow{1r} (0,1,1,1,0,0,0,0,0,1,1,0,0,1,0,0)$	5,10,14	4,6,9,13,15	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,1,1,0,0,1,1,1,1) \xrightarrow{1r} (1,0,0,0,1,1,1,1,1,0,0,1,1,0,1,0)$	5,10,14,16,17,18	4,6,9,13,15,17,18	2^{-23}
$(0,0,0,1,1,1,0,0,1,1,0,1,0,0,0,0) \xrightarrow{1r} (0,1,1,0,0,1,1,1,0,0,0,0,0,1,0,0)$	5,10,12	4,6,9	2^{-12}
$(0,0,0,1,1,1,0,0,1,1,0,1,0,0,0,1) \xrightarrow{1r} (1,0,0,1,1,0,0,0,1,1,1,1,1,0,1,0)$	5,10,12,16,17,18	4,6,9,17,18	$2^{-6.5}$
$(0,0,0,1,1,1,0,0,1,1,0,1,0,0,1,0) \xrightarrow{1r} (1,0,1,0,0,1,1,0,0,0,0,0,0,1,0,0)$	5,10,12,18	4,6,9,15,18	2^{-12}
$(0,0,0,1,1,1,0,0,1,1,0,1,0,0,1,1) \xrightarrow{1r} (0,1,0,1,1,0,0,1,1,1,1,1,1,0,1,0)$	5,10,12,16,17	4,6,9,15,17	$2^{-6.5}$
$(0,0,0,1,1,1,0,0,1,1,0,1,0,1,0,0) \xrightarrow{1r} (1,0,1,1,1,0,1,0,0,1,1,1,1,0,1,1)$	5,10,12,14,17,18	4,6,9,17,18	$2^{-6.5}$
$(0,0,0,1,1,1,0,0,1,1,0,1,0,1,0,1) \xrightarrow{1r} (0,1,0,0,0,1,0,1,1,0,0,0,0,1,0,1)$	5,10,12,14,16	4,6,9	2^{-23}
$(0,0,0,1,1,1,0,0,1,1,0,1,0,1,1,0) \xrightarrow{1r} (0,1,1,1,1,0,1,1,0,1,1,1,1,0,1,1)$	5,10,12,14,17	4,6,9,15,17	$2^{-6.5}$
$(0,0,0,1,1,1,0,0,1,1,0,1,0,1,1,1) \xrightarrow{1r} (1,0,0,0,0,1,0,0,1,0,0,0,0,1,0,1)$	5,10,12,14,16,18	4,6,9,15,18	2^{-23}
$(0,0,0,1,1,1,0,0,1,1,0,1,1,0,0,0) \xrightarrow{1r} (1,0,1,1,0,0,1,1,0,1,0,0,0,1,0,0)$	5,10,12,18	4,6,9,13,18	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,1,1,0,1,1,0,0,1) \xrightarrow{1r} (0,1,0,0,1,1,0,0,1,0,1,1,1,0,1,0)$	5,10,12,16,17	4,6,9,13,17	2^{-12}
$(0,0,0,1,1,1,0,0,1,1,0,1,1,0,0,0) \xrightarrow{1r} (0,1,1,1,0,0,1,0,0,1,0,0,0,1,0,0)$	5,10,12	4,6,9,13,15	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,1,1,0,1,1,0,1,1) \xrightarrow{1r} (1,0,0,0,1,1,0,1,1,0,1,1,1,0,1,0)$	5,10,12,16,17,18	4,6,9,13,15,17,18	2^{-12}
$(0,0,0,1,1,1,0,0,1,1,0,1,1,1,0,0) \xrightarrow{1r} (0,1,1,0,1,1,1,0,0,0,1,1,1,0,1,1)$	5,10,12,14,17	4,6,9,13,17	2^{-1}
$(0,0,0,1,1,1,0,0,1,1,0,1,1,1,0,1) \xrightarrow{1r} (1,0,0,1,0,0,0,1,1,1,0,0,0,1,0,1)$	5,10,12,14,16,18	4,6,9,13,18	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,1,1,0,1,1,1,1,0) \xrightarrow{1r} (1,0,1,0,1,1,1,1,0,0,1,1,1,0,1,1)$	5,10,12,14,17,18	4,6,9,13,15,17,18	2^{-1}
$(0,0,0,1,1,1,0,0,1,1,0,1,1,1,1,1) \xrightarrow{1r} (0,1,0,1,0,0,0,0,1,1,0,0,0,1,0,1)$	5,10,12,14,16	4,6,9,13,15	$2^{-17.5}$

Table 0.232 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,1,1,1,0,0,1,1,1,0,0,0,0,0) \xrightarrow{1r} (0,1,1,1,1,1,0,0,0,0,0,0,1,0,1,1)$	5,10,17	4,6,9,11,17	$2^{-6.5}$
$(0,0,0,1,1,1,0,0,1,1,1,0,0,0,0,1) \xrightarrow{1r} (1,0,0,0,0,0,1,1,1,1,1,0,1,0,1)$	5,10,16,18	4,6,9,11,18	2^{-12}
$(0,0,0,1,1,1,0,0,1,1,1,0,0,0,1,0) \xrightarrow{1r} (1,0,1,1,1,1,0,1,0,0,0,0,1,0,1,1)$	5,10,17,18	4,6,9,11,15,17,18	$2^{-6.5}$
$(0,0,0,1,1,1,0,0,1,1,1,0,0,0,1,1) \xrightarrow{1r} (0,1,0,0,0,0,1,0,1,1,1,1,0,1,0,1)$	5,10,16	4,6,9,11,15	2^{-12}
$(0,0,0,1,1,1,0,0,1,1,1,0,0,1,0,0) \xrightarrow{1r} (1,0,1,0,0,0,0,1,0,1,1,1,0,1,0,0)$	5,10,14,18	4,6,9,11,18	2^{-12}
$(0,0,0,1,1,1,0,0,1,1,1,0,0,1,0,1) \xrightarrow{1r} (0,1,0,1,1,1,1,0,1,0,0,0,1,0,1,0)$	5,10,14,16,17	4,6,9,11,17	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,1,1,1,0,0,1,1,0) \xrightarrow{1r} (0,1,1,0,0,0,0,0,0,1,1,1,0,1,0,0)$	5,10,14	4,6,9,11,15	2^{-12}
$(0,0,0,1,1,1,0,0,1,1,1,0,0,1,1,1) \xrightarrow{1r} (1,0,0,1,1,1,1,1,0,0,0,1,0,1,0)$	5,10,14,16,17,18	4,6,9,11,15,17,18	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,1,1,1,0,1,0,0,0) \xrightarrow{1r} (1,0,1,0,1,0,0,0,0,1,0,0,1,0,1,1)$	5,10,17,18	4,6,9,11,13,17,18	2^{-12}
$(0,0,0,1,1,1,0,0,1,1,1,0,1,0,0,1) \xrightarrow{1r} (0,1,0,1,0,1,1,1,0,1,1,0,1,0,1,0)$	5,10,16	4,6,9,11,13	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,1,1,1,0,1,0,1,0) \xrightarrow{1r} (0,1,1,0,1,0,0,1,0,1,0,0,1,0,1,1)$	5,10,17	4,6,9,11,13,15,17	2^{-12}
$(0,0,0,1,1,1,0,0,1,1,1,0,1,0,1,1) \xrightarrow{1r} (1,0,0,1,0,1,1,0,1,0,1,0,1,0,1,0)$	5,10,16,18	4,6,9,11,13,15,18	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,1,1,1,0,1,1,0,0) \xrightarrow{1r} (0,1,1,1,0,1,0,1,0,0,1,1,0,1,0,0)$	5,10,14	4,6,9,11,13	$2^{-6.5}$
$(0,0,0,1,1,1,0,0,1,1,1,0,1,1,0,1) \xrightarrow{1r} (1,0,0,0,1,0,1,0,1,1,0,0,1,0,1,0)$	5,10,14,16,17,18	4,6,9,11,13,17,18	2^{-12}
$(0,0,0,1,1,1,0,0,1,1,1,0,1,1,1,0) \xrightarrow{1r} (1,0,1,1,0,1,0,0,0,0,1,1,0,1,0,0)$	5,10,14,18	4,6,9,11,13,15,18	$2^{-6.5}$
$(0,0,0,1,1,1,0,0,1,1,1,0,1,1,1,1) \xrightarrow{1r} (0,1,0,0,1,0,1,1,1,1,0,0,1,0,1,0)$	5,10,14,16,17	4,6,9,11,13,15,17	2^{-12}
$(0,0,0,1,1,1,0,0,1,1,1,1,0,0,0,0) \xrightarrow{1r} (1,0,1,0,0,0,1,1,0,1,0,1,0,1,0,0)$	5,10,12,18	4,6,9,11,18	2^{-23}
$(0,0,0,1,1,1,0,0,1,1,1,1,0,0,0,1) \xrightarrow{1r} (0,1,0,1,1,1,0,0,1,0,1,0,1,0,1,0)$	5,10,12,16,17	4,6,9,11,17	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,1,1,1,1,0,0,1,0) \xrightarrow{1r} (0,1,1,0,0,0,1,0,0,1,0,1,0,1,0,0)$	5,10,12	4,6,9,11,15	2^{-23}
$(0,0,0,1,1,1,0,0,1,1,1,1,0,0,1,1) \xrightarrow{1r} (1,0,0,1,1,1,0,1,1,0,1,0,1,0,1,0)$	5,10,12,16,17,18	4,6,9,11,15,17,18	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,1,1,1,1,0,1,0,0) \xrightarrow{1r} (0,1,1,1,1,1,1,0,0,0,1,0,1,0,1,1)$	5,10,12,14,17	4,6,9,11,17	$2^{-6.5}$
$(0,0,0,1,1,1,0,0,1,1,1,1,0,1,0,1) \xrightarrow{1r} (1,0,0,0,0,0,0,1,1,1,0,1,0,1,0,1)$	5,10,12,14,16,18	4,6,9,11,18	2^{-23}
$(0,0,0,1,1,1,0,0,1,1,1,1,0,1,1,0) \xrightarrow{1r} (1,0,1,1,1,1,1,1,0,0,1,0,1,0,1,1)$	5,10,12,14,17,18	4,6,9,11,15,17,18	$2^{-6.5}$
$(0,0,0,1,1,1,0,0,1,1,1,1,0,1,1,1) \xrightarrow{1r} (0,1,0,0,0,0,0,0,1,1,0,1,0,1,0,1)$	5,10,12,14,16	4,6,9,11,15	2^{-23}
$(0,0,0,1,1,1,0,0,1,1,1,1,1,0,0,0) \xrightarrow{1r} (0,1,1,1,0,1,1,1,0,0,0,1,0,1,0,0)$	5,10,12	4,6,9,11,13	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,1,1,1,1,1,0,0,1) \xrightarrow{1r} (1,0,0,0,1,0,0,0,1,1,1,0,1,0,1,0)$	5,10,12,16,17,18	4,6,9,11,13,17,18	2^{-12}
$(0,0,0,1,1,1,0,0,1,1,1,1,1,0,1,0) \xrightarrow{1r} (1,0,1,1,0,1,1,0,0,0,0,1,0,1,0,0)$	5,10,12,18	4,6,9,11,13,15,18	$2^{-17.5}$
$(0,0,0,1,1,1,0,0,1,1,1,1,1,0,1,1) \xrightarrow{1r} (0,1,0,0,1,0,0,1,1,1,1,0,1,0,1,0)$	5,10,12,16,17	4,6,9,11,13,15,17	2^{-12}
$(0,0,0,1,1,1,0,0,1,1,1,1,1,1,0,0) \xrightarrow{1r} (1,0,1,0,1,0,1,0,0,1,1,0,1,0,1,1)$	5,10,12,14,17,18	4,6,9,11,13,17,18	2^{-12}
$(0,0,0,1,1,1,0,0,1,1,1,1,1,1,0,1) \xrightarrow{1r} (0,1,0,1,0,1,0,1,1,0,0,1,0,1,0,1)$	5,10,12,14,16	4,6,9,11,13	$2^{-28.5}$
$(0,0,0,1,1,1,0,0,1,1,1,1,1,1,1,0) \xrightarrow{1r} (0,1,1,0,1,0,1,1,0,1,1,0,1,0,1,1)$	5,10,12,14,17	4,6,9,11,13,15,17	2^{-12}
$(0,0,0,1,1,1,0,0,1,1,1,1,1,1,1,1) \xrightarrow{1r} (1,0,0,1,0,1,0,0,1,0,0,1,0,1,0,1)$	5,10,12,14,16,18	4,6,9,11,13,15,18	$2^{-28.5}$

Table 0.233 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	5,17	4,6,8,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	5,16,18	4,6,8,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	5,17,18	4,6,8,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	5,16	4,6,8,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	5,14,18	4,6,8,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	5,14,16,17	4,6,8,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	5,14	4,6,8,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	5,14,16,17,18	4,6,8,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	5,17,18	4,6,8,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	5,16	4,6,8,13	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	5,17	4,6,8,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	5,16,18	4,6,8,13,15,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	5,14	4,6,8,13	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	5,14,16,17,18	4,6,8,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	5,14,18	4,6,8,13,15,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	5,14,16,17	4,6,8,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	5,12,18	4,6,8,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	5,12,16,17	4,6,8,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	5,12	4,6,8,15	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	5,12,16,17,18	4,6,8,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	5,12,14,17	4,6,8,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	5,12,14,16,18	4,6,8,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	5,12,14,17,18	4,6,8,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	5,12,14,16	4,6,8,15	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	5,12	4,6,8,13	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	5,12,16,17,18	4,6,8,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	5,12,18	4,6,8,13,15,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	5,12,16,17	4,6,8,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	5,12,14,17,18	4,6,8,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	5,12,14,16	4,6,8,13	2^{-1}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	5,12,14,17	4,6,8,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	5,12,14,16,18	4,6,8,13,15,18	2^{-1}

Table 0.234 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,1,1,1,0,1,0,0,1,0,0,0,0,0) \xrightarrow{1r} (1,1,1,0,0,0,1,1,1,1,1,0,1,0,1)$	5,17,18	4,6,8,11,17,18	2^{-12}
$(0,0,0,1,1,1,0,1,0,0,1,0,0,0,0,1) \xrightarrow{1r} (0,0,0,1,1,1,0,0,0,0,0,0,1,0,1,1)$	5,16	4,6,8,11	$2^{-6.5}$
$(0,0,0,1,1,1,0,1,0,0,1,0,0,0,1,0) \xrightarrow{1r} (0,0,1,0,0,0,1,0,1,1,1,0,1,0,1)$	5,17	4,6,8,11,15,17	2^{-12}
$(0,0,0,1,1,1,0,1,0,0,1,0,0,0,1,1) \xrightarrow{1r} (1,1,0,1,1,1,0,1,0,0,0,0,1,0,1,1)$	5,16,18	4,6,8,11,15,18	$2^{-6.5}$
$(0,0,0,1,1,1,0,1,0,0,1,0,0,1,0,0) \xrightarrow{1r} (0,0,1,1,1,1,0,1,0,0,0,0,1,0,1,0)$	5,14	4,6,8,11	$2^{-17.5}$
$(0,0,0,1,1,1,0,1,0,0,1,0,0,1,0,1) \xrightarrow{1r} (1,1,0,0,0,0,0,1,0,1,1,1,0,1,0,0)$	5,14,16,17,18	4,6,8,11,17,18	2^{-12}
$(0,0,0,1,1,1,0,1,0,0,1,0,0,1,1,0) \xrightarrow{1r} (1,1,1,1,1,1,1,1,0,0,0,0,1,0,1,0)$	5,14,18	4,6,8,11,15,18	$2^{-17.5}$
$(0,0,0,1,1,1,0,1,0,0,1,0,0,1,1,1) \xrightarrow{1r} (0,0,0,0,0,0,0,0,0,0,1,1,1,0,1,0,0)$	5,14,16,17	4,6,8,11,15,17	2^{-12}
$(0,0,0,1,1,1,0,1,0,0,1,0,1,0,0,0) \xrightarrow{1r} (0,0,1,1,0,1,1,1,0,1,0,1,0,1,0,1)$	5,17	4,6,8,11,13,17	$2^{-17.5}$
$(0,0,0,1,1,1,0,1,0,0,1,0,1,0,0,1) \xrightarrow{1r} (1,1,0,0,1,0,0,0,0,1,0,0,1,0,1,1)$	5,16,18	4,6,8,11,13,18	2^{-12}
$(0,0,0,1,1,1,0,1,0,0,1,0,1,0,1,0) \xrightarrow{1r} (1,1,1,1,0,1,1,0,1,0,1,0,1,0,1,0)$	5,17,18	4,6,8,11,13,15,17,18	$2^{-17.5}$
$(0,0,0,1,1,1,0,1,0,0,1,0,1,0,1,1) \xrightarrow{1r} (0,0,0,0,1,0,0,1,0,1,0,0,1,0,1,1)$	5,16	4,6,8,11,13,15	2^{-12}
$(0,0,0,1,1,1,0,1,0,0,1,0,1,1,0,0) \xrightarrow{1r} (1,1,1,0,1,0,1,0,1,1,0,0,1,0,1,0)$	5,14,18	4,6,8,11,13,18	2^{-12}
$(0,0,0,1,1,1,0,1,0,0,1,0,1,1,0,1) \xrightarrow{1r} (0,0,0,1,0,1,0,1,0,0,0,1,1,0,1,0,0)$	5,14,16,17	4,6,8,11,13,17	$2^{-6.5}$
$(0,0,0,1,1,1,0,1,0,0,1,0,1,1,1,0) \xrightarrow{1r} (0,0,1,0,1,0,1,1,1,1,0,0,1,0,1,0)$	5,14	4,6,8,11,13,15	2^{-12}
$(0,0,0,1,1,1,0,1,0,0,1,0,1,1,1,1) \xrightarrow{1r} (1,1,0,1,0,1,0,0,0,0,1,1,0,1,0,0)$	5,14,16,17,18	4,6,8,11,13,15,17,18	$2^{-6.5}$
$(0,0,0,1,1,1,0,1,0,0,1,1,0,0,0,0) \xrightarrow{1r} (0,0,1,1,1,1,0,0,1,0,1,0,1,0,1,0)$	5,12	4,6,8,11	$2^{-17.5}$
$(0,0,0,1,1,1,0,1,0,0,1,1,0,0,0,1) \xrightarrow{1r} (1,1,0,0,0,0,1,1,0,1,0,1,0,1,0,0)$	5,12,16,17,18	4,6,8,11,17,18	2^{-23}
$(0,0,0,1,1,1,0,1,0,0,1,1,0,0,1,0) \xrightarrow{1r} (1,1,1,1,1,1,0,1,1,0,1,0,1,0,1,0)$	5,12,18	4,6,8,11,15,18	$2^{-17.5}$
$(0,0,0,1,1,1,0,1,0,0,1,1,0,0,1,1) \xrightarrow{1r} (0,0,0,0,0,0,1,0,0,1,0,1,0,1,0,0)$	5,12,16,17	4,6,8,11,15,17	2^{-23}
$(0,0,0,1,1,1,0,1,0,0,1,1,0,1,0,0) \xrightarrow{1r} (1,1,1,0,0,0,0,1,1,1,0,1,0,1,0,1)$	5,12,14,17,18	4,6,8,11,17,18	2^{-23}
$(0,0,0,1,1,1,0,1,0,0,1,1,0,1,0,1) \xrightarrow{1r} (0,0,0,1,1,1,1,0,0,0,1,0,1,0,1,1)$	5,12,14,16	4,6,8,11	$2^{-6.5}$
$(0,0,0,1,1,1,0,1,0,0,1,1,0,1,1,0) \xrightarrow{1r} (0,0,1,0,0,0,0,0,1,1,0,1,0,1,0,1)$	5,12,14,17	4,6,8,11,15,17	2^{-23}
$(0,0,0,1,1,1,0,1,0,0,1,1,0,1,1,1) \xrightarrow{1r} (1,1,0,1,1,1,1,1,0,0,1,0,1,0,1,1)$	5,12,14,16,18	4,6,8,11,15,18	$2^{-6.5}$
$(0,0,0,1,1,1,0,1,0,0,1,1,1,0,0,0) \xrightarrow{1r} (1,1,1,0,1,0,0,0,0,1,1,1,0,1,0,1,0)$	5,12,18	4,6,8,11,13,18	2^{-12}
$(0,0,0,1,1,1,0,1,0,0,1,1,1,0,0,1) \xrightarrow{1r} (0,0,0,1,0,1,1,1,0,0,0,1,0,1,0,0)$	5,12,16,17	4,6,8,11,13,17	$2^{-17.5}$
$(0,0,0,1,1,1,0,1,0,0,1,1,1,0,1,0) \xrightarrow{1r} (0,0,1,0,1,0,0,0,1,1,1,1,0,1,0,1,0)$	5,12	4,6,8,11,13,15	2^{-12}
$(0,0,0,1,1,1,0,1,0,0,1,1,1,0,1,1) \xrightarrow{1r} (1,1,0,1,0,1,1,0,0,0,0,1,0,1,0,0)$	5,12,16,17,18	4,6,8,11,13,15,17,18	$2^{-17.5}$
$(0,0,0,1,1,1,0,1,0,0,1,1,1,1,0,0) \xrightarrow{1r} (0,0,1,1,0,1,0,1,1,0,0,1,0,1,0,1)$	5,12,14,17	4,6,8,11,13,17	$2^{-28.5}$
$(0,0,0,1,1,1,0,1,0,0,1,1,1,1,0,1) \xrightarrow{1r} (1,1,0,0,1,0,1,0,0,1,1,0,1,0,1,1)$	5,12,14,16,18	4,6,8,11,13,18	2^{-12}
$(0,0,0,1,1,1,0,1,0,0,1,1,1,1,1,0) \xrightarrow{1r} (1,1,1,1,0,1,0,0,1,0,0,1,0,1,0,1)$	5,12,14,17,18	4,6,8,11,13,15,17,18	$2^{-28.5}$
$(0,0,0,1,1,1,0,1,0,0,1,1,1,1,1,1) \xrightarrow{1r} (0,0,0,0,1,0,1,1,0,1,1,0,1,0,1,1)$	5,12,14,16	4,6,8,11,13,15	2^{-12}

Table 0.235 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	5,10,18	4,6,8,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	5,10,16,17	4,6,8,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	5,10	4,6,8,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	5,10,16,17,18	4,6,8,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	5,10,14,17	4,6,8,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	5,10,14,16,18	4,6,8,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	5,10,14,17,18	4,6,8,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	5,10,14,16	4,6,8,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	5,10	4,6,8,13	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	5,10,16,17,18	4,6,8,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	5,10,18	4,6,8,13,15,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	5,10,16,17	4,6,8,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	5,10,14,17,18	4,6,8,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	5,10,14,16	4,6,8,13	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	5,10,14,17	4,6,8,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	5,10,14,16,18	4,6,8,13,15,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	5,10,12,17	4,6,8,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	5,10,12,16,18	4,6,8,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	5,10,12,17,18	4,6,8,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	5,10,12,16	4,6,8,15	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	5,10,12,14,18	4,6,8,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	5,10,12,14,16,17	4,6,8,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	5,10,12,14	4,6,8,15	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	5,10,12,14,16,17,18	4,6,8,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	5,10,12,17,18	4,6,8,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	5,10,12,16	4,6,8,13	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	5,10,12,17	4,6,8,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	5,10,12,16,18	4,6,8,13,15,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	5,10,12,14	4,6,8,13	2^{-34}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	5,10,12,14,16,17,18	4,6,8,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	5,10,12,14,18	4,6,8,13,15,18	2^{-34}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	5,10,12,14,16,17	4,6,8,13,15,17	$2^{-17.5}$

Table 0.236 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	5,10	4,6,8,11	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	5,10,16,17,18	4,6,8,11,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	5,10,18	4,6,8,11,15,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	5,10,16,17	4,6,8,11,15,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	5,10,14,17,18	4,6,8,11,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	5,10,14,16	4,6,8,11	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	5,10,14,17	4,6,8,11,15,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	5,10,14,16,18	4,6,8,11,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	5,10,18	4,6,8,11,13,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	5,10,16,17	4,6,8,11,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	5,10	4,6,8,11,13,15	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	5,10,16,17,18	4,6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	5,10,14,17	4,6,8,11,13,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	5,10,14,16,18	4,6,8,11,13,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	5,10,14,17,18	4,6,8,11,13,15,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	5,10,14,16	4,6,8,11,13,15	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	5,10,12,17,18	4,6,8,11,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	5,10,12,16	4,6,8,11	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	5,10,12,17	4,6,8,11,15,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	5,10,12,16,18	4,6,8,11,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	5,10,12,14	4,6,8,11	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	5,10,12,14,16,17,18	4,6,8,11,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	5,10,12,14,18	4,6,8,11,15,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	5,10,12,14,16,17	4,6,8,11,15,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	5,10,12,17	4,6,8,11,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	5,10,12,16,18	4,6,8,11,13,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	5,10,12,17,18	4,6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	5,10,12,16	4,6,8,11,13,15	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	5,10,12,14,18	4,6,8,11,13,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	5,10,12,14,16,17	4,6,8,11,13,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	5,10,12,14	4,6,8,11,13,15	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	5,10,12,14,16,17,18	4,6,8,11,13,15,17,18	$2^{-6.5}$

Table 0.237 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	5,17,18	4,6,8,9,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	5,16	4,6,8,9	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	5,17	4,6,8,9,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	5,16,18	4,6,8,9,15,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	5,14	4,6,8,9	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	5,14,16,17,18	4,6,8,9,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	5,14,18	4,6,8,9,15,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	5,14,16,17	4,6,8,9,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	5,17	4,6,8,9,13,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	5,16,18	4,6,8,9,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	5,17,18	4,6,8,9,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	5,16	4,6,8,9,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	5,14,18	4,6,8,9,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	5,14,16,17	4,6,8,9,13,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	5,14	4,6,8,9,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	5,14,16,17,18	4,6,8,9,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	5,12	4,6,8,9	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	5,12,16,17,18	4,6,8,9,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	5,12,18	4,6,8,9,15,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	5,12,16,17	4,6,8,9,15,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	5,12,14,17,18	4,6,8,9,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	5,12,14,16	4,6,8,9	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	5,12,14,17	4,6,8,9,15,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	5,12,14,16,18	4,6,8,9,15,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	5,12,18	4,6,8,9,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	5,12,16,17	4,6,8,9,13,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	5,12	4,6,8,9,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	5,12,16,17,18	4,6,8,9,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	5,12,14,17	4,6,8,9,13,17	2^{-34}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	5,12,14,16,18	4,6,8,9,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	5,12,14,17,18	4,6,8,9,13,15,17,18	2^{-34}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	5,12,14,16	4,6,8,9,13,15	$2^{-17.5}$

Table 0.238 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	5,17	4,6,8,9,11,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	5,16,18	4,6,8,9,11,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	5,17,18	4,6,8,9,11,15,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	5,16	4,6,8,9,11,15	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	5,14,18	4,6,8,9,11,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	5,14,16,17	4,6,8,9,11,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	5,14	4,6,8,9,11,15	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	5,14,16,17,18	4,6,8,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	5,17,18	4,6,8,9,11,13,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	5,16	4,6,8,9,11,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	5,17	4,6,8,9,11,13,15,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	5,16,18	4,6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	5,14	4,6,8,9,11,13	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	5,14,16,17,18	4,6,8,9,11,13,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	5,14,18	4,6,8,9,11,13,15,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	5,14,16,17	4,6,8,9,11,13,15,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	5,12,18	4,6,8,9,11,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	5,12,16,17	4,6,8,9,11,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	5,12	4,6,8,9,11,15	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	5,12,16,17,18	4,6,8,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	5,12,14,17	4,6,8,9,11,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	5,12,14,16,18	4,6,8,9,11,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	5,12,14,17,18	4,6,8,9,11,15,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	5,12,14,16	4,6,8,9,11,15	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	5,12	4,6,8,9,11,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	5,12,16,17,18	4,6,8,9,11,13,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	5,12,18	4,6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	5,12,16,17	4,6,8,9,11,13,15,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	5,12,14,17,18	4,6,8,9,11,13,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	5,12,14,16	4,6,8,9,11,13	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	5,12,14,17	4,6,8,9,11,13,15,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	5,12,14,16,18	4,6,8,9,11,13,15,18	$2^{-6.5}$

Table 0.239 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	5,10	4,6,8,9	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	5,10,16,17,18	4,6,8,9,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	5,10,18	4,6,8,9,15,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	5,10,16,17	4,6,8,9,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	5,10,14,17,18	4,6,8,9,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	5,10,14,16	4,6,8,9	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	5,10,14,17	4,6,8,9,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	5,10,14,16,18	4,6,8,9,15,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	5,10,18	4,6,8,9,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	5,10,16,17	4,6,8,9,13,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	5,10	4,6,8,9,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	5,10,16,17,18	4,6,8,9,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	5,10,14,17	4,6,8,9,13,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	5,10,14,16,18	4,6,8,9,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	5,10,14,17,18	4,6,8,9,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	5,10,14,16	4,6,8,9,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	5,10,12,17,18	4,6,8,9,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	5,10,12,16	4,6,8,9	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	5,10,12,17	4,6,8,9,15,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	5,10,12,16,18	4,6,8,9,15,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	5,10,12,14	4,6,8,9	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	5,10,12,14,16,17,18	4,6,8,9,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	5,10,12,14,18	4,6,8,9,15,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	5,10,12,14,16,17	4,6,8,9,15,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	5,10,12,17	4,6,8,9,13,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	5,10,12,16,18	4,6,8,9,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	5,10,12,17,18	4,6,8,9,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	5,10,12,16	4,6,8,9,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	5,10,12,14,18	4,6,8,9,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	5,10,12,14,16,17	4,6,8,9,13,17	2^{-1}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	5,10,12,14	4,6,8,9,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	5,10,12,14,16,17,18	4,6,8,9,13,15,17,18	2^{-1}

Table 0.240 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	5,10,18	4,6,8,9,11,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	5,10,16,17	4,6,8,9,11,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	5,10	4,6,8,9,11,15	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	5,10,16,17,18	4,6,8,9,11,15,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	5,10,14,17	4,6,8,9,11,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	5,10,14,16,18	4,6,8,9,11,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	5,10,14,17,18	4,6,8,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	5,10,14,16	4,6,8,9,11,15	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	5,10	4,6,8,9,11,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	5,10,16,17,18	4,6,8,9,11,13,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	5,10,18	4,6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	5,10,16,17	4,6,8,9,11,13,15,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	5,10,14,17,18	4,6,8,9,11,13,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	5,10,14,16	4,6,8,9,11,13	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	5,10,14,17	4,6,8,9,11,13,15,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	5,10,14,16,18	4,6,8,9,11,13,15,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	5,10,12,17	4,6,8,9,11,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	5,10,12,16,18	4,6,8,9,11,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	5,10,12,17,18	4,6,8,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	5,10,12,16	4,6,8,9,11,15	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	5,10,12,14,18	4,6,8,9,11,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	5,10,12,14,16,17	4,6,8,9,11,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	5,10,12,14	4,6,8,9,11,15	2^{-23}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	5,10,12,14,16,17,18	4,6,8,9,11,15,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	5,10,12,17,18	4,6,8,9,11,13,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	5,10,12,16	4,6,8,9,11,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	5,10,12,17	4,6,8,9,11,13,15,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	5,10,12,16,18	4,6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	5,10,12,14	4,6,8,9,11,13	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	5,10,12,14,16,17,18	4,6,8,9,11,13,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	5,10,12,14,18	4,6,8,9,11,13,15,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	5,10,12,14,16,17	4,6,8,9,11,13,15,17	2^{-12}

Table 0.241 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	5,7	4,6	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	5,7,16,17,18	4,6,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	5,7,18	4,6,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	5,7,16,17	4,6,15,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	5,7,14,17,18	4,6,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	5,7,14,16	4,6	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	5,7,14,17	4,6,15,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	5,7,14,16,18	4,6,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	5,7,18	4,6,13,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	5,7,16,17	4,6,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	5,7	4,6,13,15	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	5,7,16,17,18	4,6,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	5,7,14,17	4,6,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	5,7,14,16,18	4,6,13,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	5,7,14,17,18	4,6,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	5,7,14,16	4,6,13,15	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	5,7,12,17,18	4,6,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	5,7,12,16	4,6	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	5,7,12,17	4,6,15,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	5,7,12,16,18	4,6,15,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	5,7,12,14	4,6	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	5,7,12,14,16,17,18	4,6,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	5,7,12,14,18	4,6,15,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	5,7,12,14,16,17	4,6,15,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	5,7,12,17	4,6,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	5,7,12,16,18	4,6,13,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	5,7,12,17,18	4,6,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	5,7,12,16	4,6,13,15	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	5,7,12,14,18	4,6,13,18	2^{-1}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	5,7,12,14,16,17	4,6,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	5,7,12,14	4,6,13,15	2^{-1}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	5,7,12,14,16,17,18	4,6,13,15,17,18	$2^{-17.5}$

Table 0.242 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	5,7,18	4,6,11,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	5,7,16,17	4,6,11,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	5,7	4,6,11,15	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	5,7,16,17,18	4,6,11,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	5,7,14,17	4,6,11,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	5,7,14,16,18	4,6,11,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	5,7,14,17,18	4,6,11,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	5,7,14,16	4,6,11,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	5,7	4,6,11,13	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	5,7,16,17,18	4,6,11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	5,7,18	4,6,11,13,15,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	5,7,16,17	4,6,11,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	5,7,14,17,18	4,6,11,13,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	5,7,14,16	4,6,11,13	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	5,7,14,17	4,6,11,13,15,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	5,7,14,16,18	4,6,11,13,15,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	5,7,12,17	4,6,11,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	5,7,12,16,18	4,6,11,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	5,7,12,17,18	4,6,11,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	5,7,12,16	4,6,11,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	5,7,12,14,18	4,6,11,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	5,7,12,14,16,17	4,6,11,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	5,7,12,14	4,6,11,15	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	5,7,12,14,16,17,18	4,6,11,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	5,7,12,17,18	4,6,11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	5,7,12,16	4,6,11,13	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	5,7,12,17	4,6,11,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	5,7,12,16,18	4,6,11,13,15,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	5,7,12,14	4,6,11,13	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	5,7,12,14,16,17,18	4,6,11,13,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	5,7,12,14,18	4,6,11,13,15,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	5,7,12,14,16,17	4,6,11,13,15,17	$2^{-28.5}$

Table 0.243 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,1,1,1,1,0,0,1,0,0,0,0,0,0) \xrightarrow{1r} (1,1,1,0,1,1,0,1,0,0,0,0,1,0,1,1)$	5,7,10,17,18	4,6,17,18	2^{-12}
$(0,0,0,1,1,1,1,0,0,1,0,0,0,0,0,1) \xrightarrow{1r} (0,0,0,1,0,0,1,0,1,1,1,1,0,1,0,1)$	5,7,10,16	4,6	$2^{-17.5}$
$(0,0,0,1,1,1,1,0,0,1,0,0,0,0,1,0) \xrightarrow{1r} (0,0,1,0,1,1,0,0,0,0,0,0,1,0,1,1)$	5,7,10,17	4,6,15,17	2^{-12}
$(0,0,0,1,1,1,1,0,0,1,0,0,0,0,1,1) \xrightarrow{1r} (1,1,0,1,0,0,1,1,1,1,1,1,0,1,0,1)$	5,7,10,16,18	4,6,15,18	$2^{-17.5}$
$(0,0,0,1,1,1,1,0,0,1,0,0,0,1,0,0) \xrightarrow{1r} (0,0,1,1,0,0,0,0,0,1,1,1,0,1,0,0)$	5,7,10,14	4,6	$2^{-17.5}$
$(0,0,0,1,1,1,1,0,0,1,0,0,0,1,0,1) \xrightarrow{1r} (1,1,0,0,1,1,1,1,1,0,0,0,1,0,1,0)$	5,7,10,14,16,17,18	4,6,17,18	2^{-23}
$(0,0,0,1,1,1,1,0,0,1,0,0,0,1,1,0) \xrightarrow{1r} (1,1,1,1,0,0,0,1,0,1,1,1,0,1,0,0)$	5,7,10,14,18	4,6,15,18	$2^{-17.5}$
$(0,0,0,1,1,1,1,0,0,1,0,0,0,1,1,1) \xrightarrow{1r} (0,0,0,0,1,1,1,0,1,0,0,0,1,0,1,0)$	5,7,10,14,16,17	4,6,15,17	2^{-23}
$(0,0,0,1,1,1,1,0,0,1,0,0,1,0,0,0) \xrightarrow{1r} (0,0,1,1,1,0,0,1,0,1,0,1,0,1,0,1)$	5,7,10,17	4,6,13,17	$2^{-17.5}$
$(0,0,0,1,1,1,1,0,0,1,0,0,1,0,0,1) \xrightarrow{1r} (1,1,0,0,0,1,1,0,1,0,1,0,1,0,1,0)$	5,7,10,16,18	4,6,13,18	2^{-23}
$(0,0,0,1,1,1,1,0,0,1,0,0,1,0,1,0) \xrightarrow{1r} (1,1,1,1,1,0,0,0,0,1,0,0,1,0,1,1)$	5,7,10,17,18	4,6,13,15,17,18	$2^{-17.5}$
$(0,0,0,1,1,1,1,0,0,1,0,0,1,0,1,1) \xrightarrow{1r} (0,0,0,0,0,1,1,1,1,0,1,1,0,1,0,1)$	5,7,10,16	4,6,13,15	2^{-23}
$(0,0,0,1,1,1,1,0,0,1,0,0,1,1,0,0) \xrightarrow{1r} (1,1,1,0,0,1,0,0,0,0,1,1,0,1,0,0)$	5,7,10,14,18	4,6,13,18	2^{-12}
$(0,0,0,1,1,1,1,0,0,1,0,0,1,1,0,1) \xrightarrow{1r} (0,0,0,1,1,0,1,1,1,1,0,0,1,0,1,0)$	5,7,10,14,16,17	4,6,13,17	$2^{-17.5}$
$(0,0,0,1,1,1,1,0,0,1,0,0,1,1,1,0) \xrightarrow{1r} (0,0,1,0,0,1,0,1,0,0,1,1,0,1,0,0)$	5,7,10,14	4,6,13,15	2^{-12}
$(0,0,0,1,1,1,1,0,0,1,0,0,1,1,1,1) \xrightarrow{1r} (1,1,0,1,1,0,1,0,1,1,0,0,1,0,1,0)$	5,7,10,14,16,17,18	4,6,13,15,17,18	$2^{-17.5}$
$(0,0,0,1,1,1,1,0,0,1,0,1,0,0,0,0) \xrightarrow{1r} (0,0,1,1,0,0,1,0,0,1,0,1,0,1,0,0)$	5,7,10,12	4,6	$2^{-28.5}$
$(0,0,0,1,1,1,1,0,0,1,0,1,0,0,0,1) \xrightarrow{1r} (1,1,0,0,1,1,0,1,1,0,1,0,1,0,1,0)$	5,7,10,12,16,17,18	4,6,17,18	2^{-23}
$(0,0,0,1,1,1,1,0,0,1,0,1,0,0,1,0) \xrightarrow{1r} (1,1,1,1,0,0,1,1,0,1,0,1,0,1,0,0)$	5,7,10,12,18	4,6,15,18	$2^{-28.5}$
$(0,0,0,1,1,1,1,0,0,1,0,1,0,0,1,1) \xrightarrow{1r} (0,0,0,0,1,1,0,0,1,0,1,0,1,0,1,0)$	5,7,10,12,16,17	4,6,15,17	2^{-23}
$(0,0,0,1,1,1,1,0,0,1,0,1,0,1,0,0) \xrightarrow{1r} (1,1,1,0,1,1,1,1,0,0,1,0,1,0,1,1)$	5,7,10,12,14,17,18	4,6,17,18	2^{-12}
$(0,0,0,1,1,1,1,0,0,1,0,1,0,1,0,1) \xrightarrow{1r} (0,0,0,1,0,0,0,0,1,1,0,1,0,1,0,1)$	5,7,10,12,14,16	4,6	$2^{-28.5}$
$(0,0,0,1,1,1,1,0,0,1,0,1,0,1,1,0) \xrightarrow{1r} (0,0,1,0,1,1,1,0,0,0,1,0,1,0,1,1)$	5,7,10,12,14,17	4,6,15,17	2^{-12}
$(0,0,0,1,1,1,1,0,0,1,0,1,0,1,1,1) \xrightarrow{1r} (1,1,0,1,0,0,0,1,1,1,0,1,0,1,0,1)$	5,7,10,12,14,16,18	4,6,15,18	$2^{-28.5}$
$(0,0,0,1,1,1,1,0,0,1,0,1,1,0,0,0) \xrightarrow{1r} (1,1,1,0,0,1,1,0,0,0,0,1,0,1,0,0)$	5,7,10,12,18	4,6,13,18	2^{-23}
$(0,0,0,1,1,1,1,0,0,1,0,1,1,0,0,1) \xrightarrow{1r} (0,0,0,1,1,0,0,1,1,1,1,0,1,0,1,0)$	5,7,10,12,16,17	4,6,13,17	$2^{-17.5}$
$(0,0,0,1,1,1,1,0,0,1,0,1,1,0,1,0) \xrightarrow{1r} (0,0,1,0,0,1,1,1,0,0,0,1,0,1,0,0)$	5,7,10,12	4,6,13,15	2^{-23}
$(0,0,0,1,1,1,1,0,0,1,0,1,1,0,1,1) \xrightarrow{1r} (1,1,0,1,1,0,0,0,1,1,1,0,1,0,1,0)$	5,7,10,12,16,17,18	4,6,13,15,17,18	$2^{-17.5}$
$(0,0,0,1,1,1,1,0,0,1,0,1,1,1,0,0) \xrightarrow{1r} (0,0,1,1,1,0,1,1,0,1,1,0,1,0,1,1)$	5,7,10,12,14,17	4,6,13,17	$2^{-17.5}$
$(0,0,0,1,1,1,1,0,0,1,0,1,1,1,0,1) \xrightarrow{1r} (1,1,0,0,0,1,0,0,1,0,0,1,0,1,0,1)$	5,7,10,12,14,16,18	4,6,13,18	2^{-34}
$(0,0,0,1,1,1,1,0,0,1,0,1,1,1,1,0) \xrightarrow{1r} (1,1,1,1,1,0,1,0,0,1,1,0,1,0,1,1)$	5,7,10,12,14,17,18	4,6,13,15,17,18	$2^{-17.5}$
$(0,0,0,1,1,1,1,0,0,1,0,1,1,1,1,1) \xrightarrow{1r} (0,0,0,0,0,1,0,1,1,0,0,1,0,1,0,1)$	5,7,10,12,14,16	4,6,13,15	2^{-34}

Table 0.244 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	5,7,10,17	4,6,11,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	5,7,10,16,18	4,6,11,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	5,7,10,17,18	4,6,11,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	5,7,10,16	4,6,11,15	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	5,7,10,14,18	4,6,11,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	5,7,10,14,16,17	4,6,11,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	5,7,10,14	4,6,11,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	5,7,10,14,16,17,18	4,6,11,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	5,7,10,17,18	4,6,11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	5,7,10,16	4,6,11,13	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	5,7,10,17	4,6,11,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	5,7,10,16,18	4,6,11,13,15,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	5,7,10,14	4,6,11,13	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	5,7,10,14,16,17,18	4,6,11,13,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	5,7,10,14,18	4,6,11,13,15,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	5,7,10,14,16,17	4,6,11,13,15,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	5,7,10,12,18	4,6,11,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	5,7,10,12,16,17	4,6,11,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	5,7,10,12	4,6,11,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	5,7,10,12,16,17,18	4,6,11,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	5,7,10,12,14,17	4,6,11,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	5,7,10,12,14,16,18	4,6,11,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	5,7,10,12,14,17,18	4,6,11,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	5,7,10,12,14,16	4,6,11,15	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	5,7,10,12	4,6,11,13	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	5,7,10,12,16,17,18	4,6,11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	5,7,10,12,18	4,6,11,13,15,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	5,7,10,12,16,17	4,6,11,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	5,7,10,12,14,17,18	4,6,11,13,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	5,7,10,12,14,16	4,6,11,13	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	5,7,10,12,14,17	4,6,11,13,15,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	5,7,10,12,14,16,18	4,6,11,13,15,18	2^{-23}

Table 0.245 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	5,7,18	4,6,9,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	5,7,16,17	4,6,9,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	5,7	4,6,9,15	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	5,7,16,17,18	4,6,9,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	5,7,14,17	4,6,9,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	5,7,14,16,18	4,6,9,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	5,7,14,17,18	4,6,9,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	5,7,14,16	4,6,9,15	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	5,7	4,6,9,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	5,7,16,17,18	4,6,9,13,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	5,7,18	4,6,9,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	5,7,16,17	4,6,9,13,15,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	5,7,14,17,18	4,6,9,13,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	5,7,14,16	4,6,9,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	5,7,14,17	4,6,9,13,15,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	5,7,14,16,18	4,6,9,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	5,7,12,17	4,6,9,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	5,7,12,16,18	4,6,9,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	5,7,12,17,18	4,6,9,15,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	5,7,12,16	4,6,9,15	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	5,7,12,14,18	4,6,9,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	5,7,12,14,16,17	4,6,9,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	5,7,12,14	4,6,9,15	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	5,7,12,14,16,17,18	4,6,9,15,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	5,7,12,17,18	4,6,9,13,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	5,7,12,16	4,6,9,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	5,7,12,17	4,6,9,13,15,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	5,7,12,16,18	4,6,9,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	5,7,12,14	4,6,9,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	5,7,12,14,16,17,18	4,6,9,13,17,18	2^{-34}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	5,7,12,14,18	4,6,9,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	5,7,12,14,16,17	4,6,9,13,15,17	2^{-34}

Table 0.246 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,1,1,1,1,0,1,0,1,0,0,0,0,0) \xrightarrow{1r} (0,1,0,0,1,0,0,1,0,1,0,1,1,0,0,0)$	5,7	4,6,9,11	2^{-23}
$(0,0,0,1,1,1,1,0,1,0,1,0,0,0,0,1) \xrightarrow{1r} (1,0,1,1,0,1,1,0,1,0,1,0,0,1,1,0)$	5,7,16,17,18	4,6,9,11,17,18	$2^{-28.5}$
$(0,0,0,1,1,1,1,0,1,0,1,0,0,0,1,0) \xrightarrow{1r} (1,0,0,0,1,0,0,0,0,1,0,1,1,0,0,0)$	5,7,18	4,6,9,11,15,18	2^{-23}
$(0,0,0,1,1,1,1,0,1,0,1,0,0,0,1,1) \xrightarrow{1r} (0,1,1,1,0,1,1,1,1,0,1,0,0,1,1,0)$	5,7,16,17	4,6,9,11,15,17	$2^{-28.5}$
$(0,0,0,1,1,1,1,0,1,0,1,0,0,1,0,0) \xrightarrow{1r} (1,0,0,1,0,1,0,0,0,0,1,0,0,1,1,1)$	5,7,14,17,18	4,6,9,11,17,18	$2^{-17.5}$
$(0,0,0,1,1,1,1,0,1,0,1,0,0,1,0,1) \xrightarrow{1r} (0,1,1,0,1,0,1,1,1,1,0,1,1,0,0,1)$	5,7,14,16	4,6,9,11	2^{-23}
$(0,0,0,1,1,1,1,0,1,0,1,0,0,1,1,0) \xrightarrow{1r} (0,1,0,1,0,1,0,1,0,0,1,0,0,1,1,1)$	5,7,14,17	4,6,9,11,15,17	$2^{-17.5}$
$(0,0,0,1,1,1,1,0,1,0,1,0,0,1,1,1) \xrightarrow{1r} (1,0,1,0,1,0,1,0,1,1,0,1,1,0,0,1)$	5,7,14,16,18	4,6,9,11,15,18	2^{-23}
$(0,0,0,1,1,1,1,0,1,0,1,0,1,0,0,0) \xrightarrow{1r} (1,0,0,1,1,1,0,1,0,0,0,1,1,0,0,0)$	5,7,18	4,6,9,11,13,18	$2^{-17.5}$
$(0,0,0,1,1,1,1,0,1,0,1,0,1,0,0,1) \xrightarrow{1r} (0,1,1,0,0,0,1,0,1,1,1,0,0,1,1,0)$	5,7,16,17	4,6,9,11,13,17	2^{-23}
$(0,0,0,1,1,1,1,0,1,0,1,0,1,0,1,0) \xrightarrow{1r} (0,1,0,1,1,1,0,0,0,0,0,1,1,0,0,0)$	5,7	4,6,9,11,13,15	$2^{-17.5}$
$(0,0,0,1,1,1,1,0,1,0,1,0,1,0,1,1) \xrightarrow{1r} (1,0,1,0,0,0,1,1,1,1,1,0,0,1,1,0)$	5,7,16,17,18	4,6,9,11,13,15,17,18	2^{-23}
$(0,0,0,1,1,1,1,0,1,0,1,0,1,1,0,0) \xrightarrow{1r} (0,1,0,0,0,0,0,0,0,1,1,0,0,1,1,1)$	5,7,14,17	4,6,9,11,13,17	2^{-23}
$(0,0,0,1,1,1,1,0,1,0,1,0,1,1,0,1) \xrightarrow{1r} (1,0,1,1,1,1,1,1,1,0,0,1,1,0,0,1)$	5,7,14,16,18	4,6,9,11,13,18	$2^{-28.5}$
$(0,0,0,1,1,1,1,0,1,0,1,0,1,1,1,0) \xrightarrow{1r} (1,0,0,0,0,0,0,1,0,1,1,0,0,1,1,1)$	5,7,14,17,18	4,6,9,11,13,15,17,18	2^{-23}
$(0,0,0,1,1,1,1,0,1,0,1,0,1,1,1,1) \xrightarrow{1r} (0,1,1,1,1,1,1,0,1,0,0,1,1,0,0,1)$	5,7,14,16	4,6,9,11,13,15	$2^{-28.5}$
$(0,0,0,1,1,1,1,0,1,0,1,1,0,0,0,0) \xrightarrow{1r} (1,0,0,1,0,1,1,0,0,0,0,0,0,1,1,1)$	5,7,12,17,18	4,6,9,11,17,18	$2^{-17.5}$
$(0,0,0,1,1,1,1,0,1,0,1,1,0,0,0,1) \xrightarrow{1r} (0,1,1,0,1,0,0,1,1,1,1,1,1,0,0,1)$	5,7,12,16	4,6,9,11	2^{-12}
$(0,0,0,1,1,1,1,0,1,0,1,1,0,0,1,0) \xrightarrow{1r} (0,1,0,1,0,1,1,1,0,0,0,0,0,1,1,1)$	5,7,12,17	4,6,9,11,15,17	$2^{-17.5}$
$(0,0,0,1,1,1,1,0,1,0,1,1,0,0,1,1) \xrightarrow{1r} (1,0,1,0,1,0,0,0,1,1,1,1,1,0,0,1)$	5,7,12,16,18	4,6,9,11,15,18	2^{-12}
$(0,0,0,1,1,1,1,0,1,0,1,1,0,1,0,0) \xrightarrow{1r} (0,1,0,0,1,0,1,1,0,1,1,1,1,0,0,0)$	5,7,12,14	4,6,9,11	2^{-12}
$(0,0,0,1,1,1,1,0,1,0,1,1,0,1,0,1) \xrightarrow{1r} (1,0,1,1,0,1,0,0,1,0,0,0,0,1,1,0)$	5,7,12,14,16,17,18	4,6,9,11,17,18	$2^{-28.5}$
$(0,0,0,1,1,1,1,0,1,0,1,1,0,1,1,0) \xrightarrow{1r} (1,0,0,0,1,0,1,0,0,1,1,1,1,0,0,0)$	5,7,12,14,18	4,6,9,11,15,18	2^{-12}
$(0,0,0,1,1,1,1,0,1,0,1,1,0,1,1,1) \xrightarrow{1r} (0,1,1,1,0,1,0,1,1,0,0,0,0,1,1,0)$	5,7,12,14,16,17	4,6,9,11,15,17	$2^{-28.5}$
$(0,0,0,1,1,1,1,0,1,0,1,1,1,0,0,0) \xrightarrow{1r} (0,1,0,0,0,0,1,0,0,1,0,0,0,1,1,1)$	5,7,12,17	4,6,9,11,13,17	2^{-23}
$(0,0,0,1,1,1,1,0,1,0,1,1,1,0,0,1) \xrightarrow{1r} (1,0,1,1,1,1,0,1,1,0,1,1,1,0,0,1)$	5,7,12,16,18	4,6,9,11,13,18	$2^{-17.5}$
$(0,0,0,1,1,1,1,0,1,0,1,1,1,0,1,0) \xrightarrow{1r} (1,0,0,0,0,0,1,1,0,1,0,0,0,1,1,1)$	5,7,12,17,18	4,6,9,11,13,15,17,18	2^{-23}
$(0,0,0,1,1,1,1,0,1,0,1,1,1,0,1,1) \xrightarrow{1r} (0,1,1,1,1,1,0,0,1,0,1,1,1,0,0,1)$	5,7,12,16	4,6,9,11,13,15	$2^{-17.5}$
$(0,0,0,1,1,1,1,0,1,0,1,1,1,1,0,0) \xrightarrow{1r} (1,0,0,1,1,1,1,1,0,0,1,1,1,0,0,0)$	5,7,12,14,18	4,6,9,11,13,18	$2^{-6.5}$
$(0,0,0,1,1,1,1,0,1,0,1,1,1,1,0,1) \xrightarrow{1r} (0,1,1,0,0,0,0,0,1,1,0,0,0,1,1,0)$	5,7,12,14,16,17	4,6,9,11,13,17	2^{-23}
$(0,0,0,1,1,1,1,0,1,0,1,1,1,1,1,0) \xrightarrow{1r} (0,1,0,1,1,1,1,0,0,0,1,1,1,0,0,0)$	5,7,12,14	4,6,9,11,13,15	$2^{-6.5}$
$(0,0,0,1,1,1,1,0,1,0,1,1,1,1,1,1) \xrightarrow{1r} (1,0,1,0,0,0,0,1,1,1,0,0,0,1,1,0)$	5,7,12,14,16,17,18	4,6,9,11,13,15,17,18	2^{-23}

Table 0.247 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	5,7,10,17	4,6,9,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	5,7,10,16,18	4,6,9,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	5,7,10,17,18	4,6,9,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	5,7,10,16	4,6,9,15	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	5,7,10,14,18	4,6,9,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	5,7,10,14,16,17	4,6,9,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	5,7,10,14	4,6,9,15	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	5,7,10,14,16,17,18	4,6,9,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	5,7,10,17,18	4,6,9,13,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	5,7,10,16	4,6,9,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	5,7,10,17	4,6,9,13,15,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	5,7,10,16,18	4,6,9,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	5,7,10,14	4,6,9,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	5,7,10,14,16,17,18	4,6,9,13,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	5,7,10,14,18	4,6,9,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	5,7,10,14,16,17	4,6,9,13,15,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	5,7,10,12,18	4,6,9,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	5,7,10,12,16,17	4,6,9,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	5,7,10,12	4,6,9,15	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	5,7,10,12,16,17,18	4,6,9,15,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	5,7,10,12,14,17	4,6,9,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	5,7,10,12,14,16,18	4,6,9,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	5,7,10,12,14,17,18	4,6,9,15,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	5,7,10,12,14,16	4,6,9,15	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	5,7,10,12	4,6,9,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	5,7,10,12,16,17,18	4,6,9,13,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	5,7,10,12,18	4,6,9,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	5,7,10,12,16,17	4,6,9,13,15,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	5,7,10,12,14,17,18	4,6,9,13,17,18	2^{-1}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	5,7,10,12,14,16	4,6,9,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	5,7,10,12,14,17	4,6,9,13,15,17	2^{-1}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	5,7,10,12,14,16,18	4,6,9,13,15,18	$2^{-17.5}$

Table 0.248 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,1,1,1,1,0,1,1,1,0,0,0,0,0) \xrightarrow{1r} (1,0,1,1,1,1,0,0,0,0,0,0,1,1,1,1)$	5,7,10,17,18	4,6,9,11,17,18	$2^{-6.5}$
$(0,0,0,1,1,1,1,0,1,1,1,0,0,0,0,1) \xrightarrow{1r} (0,1,0,0,0,0,1,1,1,1,1,0,0,0,1)$	5,7,10,16	4,6,9,11	2^{-12}
$(0,0,0,1,1,1,1,0,1,1,1,0,0,0,1,0) \xrightarrow{1r} (0,1,1,1,1,1,0,1,0,0,0,0,1,1,1,1)$	5,7,10,17	4,6,9,11,15,17	$2^{-6.5}$
$(0,0,0,1,1,1,1,0,1,1,1,0,0,0,1,1) \xrightarrow{1r} (1,0,0,0,0,0,1,0,1,1,1,1,0,0,0,1)$	5,7,10,16,18	4,6,9,11,15,18	2^{-12}
$(0,0,0,1,1,1,1,0,1,1,1,0,0,1,0,0) \xrightarrow{1r} (0,1,1,0,0,0,0,1,0,1,1,1,0,0,0,0)$	5,7,10,14	4,6,9,11	2^{-12}
$(0,0,0,1,1,1,1,0,1,1,1,0,0,1,0,1) \xrightarrow{1r} (1,0,0,1,1,1,1,0,1,0,0,0,1,1,1,0)$	5,7,10,14,16,17,18	4,6,9,11,17,18	$2^{-17.5}$
$(0,0,0,1,1,1,1,0,1,1,1,0,0,1,1,0) \xrightarrow{1r} (1,0,1,0,0,0,0,0,0,1,1,1,0,0,0,0)$	5,7,10,14,18	4,6,9,11,15,18	2^{-12}
$(0,0,0,1,1,1,1,0,1,1,1,0,0,1,1,1) \xrightarrow{1r} (0,1,0,1,1,1,1,1,1,0,0,0,1,1,1,0)$	5,7,10,14,16,17	4,6,9,11,15,17	$2^{-17.5}$
$(0,0,0,1,1,1,1,0,1,1,1,0,1,0,0,0) \xrightarrow{1r} (0,1,1,0,1,0,0,0,0,1,0,0,1,1,1,1)$	5,7,10,17	4,6,9,11,13,17	2^{-12}
$(0,0,0,1,1,1,1,0,1,1,1,0,1,0,0,1) \xrightarrow{1r} (1,0,0,1,0,1,1,1,1,0,1,0,0,0,1)$	5,7,10,16,18	4,6,9,11,13,18	$2^{-17.5}$
$(0,0,0,1,1,1,1,0,1,1,1,0,1,0,1,0) \xrightarrow{1r} (1,0,1,0,1,0,0,1,0,1,0,0,1,1,1,1)$	5,7,10,17,18	4,6,9,11,13,15,17,18	2^{-12}
$(0,0,0,1,1,1,1,0,1,1,1,0,1,0,1,1) \xrightarrow{1r} (0,1,0,1,0,1,1,0,1,0,1,1,0,0,0,1)$	5,7,10,16	4,6,9,11,13,15	$2^{-17.5}$
$(0,0,0,1,1,1,1,0,1,1,1,0,1,1,0,0) \xrightarrow{1r} (1,0,1,1,0,1,0,1,0,0,1,1,0,0,0,0)$	5,7,10,14,18	4,6,9,11,13,18	$2^{-6.5}$
$(0,0,0,1,1,1,1,0,1,1,1,0,1,1,0,1) \xrightarrow{1r} (0,1,0,0,1,0,1,0,1,1,0,0,1,1,1,0)$	5,7,10,14,16,17	4,6,9,11,13,17	2^{-12}
$(0,0,0,1,1,1,1,0,1,1,1,0,1,1,1,0) \xrightarrow{1r} (0,1,1,1,0,1,0,0,0,0,1,1,0,0,0,0)$	5,7,10,14	4,6,9,11,13,15	$2^{-6.5}$
$(0,0,0,1,1,1,1,0,1,1,1,0,1,1,1,1) \xrightarrow{1r} (1,0,0,0,1,0,1,1,1,1,0,0,1,1,1,0)$	5,7,10,14,16,17,18	4,6,9,11,13,15,17,18	2^{-12}
$(0,0,0,1,1,1,1,0,1,1,1,1,0,0,0,0) \xrightarrow{1r} (0,1,1,0,0,0,1,1,0,1,0,1,0,0,0,0)$	5,7,10,12	4,6,9,11	2^{-23}
$(0,0,0,1,1,1,1,0,1,1,1,1,0,0,0,1) \xrightarrow{1r} (1,0,0,1,1,1,0,0,1,0,1,0,1,1,1,0)$	5,7,10,12,16,17,18	4,6,9,11,17,18	$2^{-17.5}$
$(0,0,0,1,1,1,1,0,1,1,1,1,0,0,1,0) \xrightarrow{1r} (1,0,1,0,0,0,1,0,0,1,0,1,0,0,0,0)$	5,7,10,12,18	4,6,9,11,15,18	2^{-23}
$(0,0,0,1,1,1,1,0,1,1,1,1,0,0,1,1) \xrightarrow{1r} (0,1,0,1,1,1,0,1,1,0,1,0,1,1,1,0)$	5,7,10,12,16,17	4,6,9,11,15,17	$2^{-17.5}$
$(0,0,0,1,1,1,1,0,1,1,1,1,0,1,0,0) \xrightarrow{1r} (1,0,1,1,1,1,1,0,0,0,1,0,1,1,1,1)$	5,7,10,12,14,17,18	4,6,9,11,17,18	$2^{-6.5}$
$(0,0,0,1,1,1,1,0,1,1,1,1,0,1,0,1) \xrightarrow{1r} (0,1,0,0,0,0,0,1,1,1,0,1,0,0,0,1)$	5,7,10,12,14,16	4,6,9,11	2^{-23}
$(0,0,0,1,1,1,1,0,1,1,1,1,0,1,1,0) \xrightarrow{1r} (0,1,1,1,1,1,1,1,0,0,1,0,1,1,1,1)$	5,7,10,12,14,17	4,6,9,11,15,17	$2^{-6.5}$
$(0,0,0,1,1,1,1,0,1,1,1,1,0,1,1,1) \xrightarrow{1r} (1,0,0,0,0,0,0,0,1,1,0,1,0,0,0,1)$	5,7,10,12,14,16,18	4,6,9,11,15,18	2^{-23}
$(0,0,0,1,1,1,1,0,1,1,1,1,1,0,0,0) \xrightarrow{1r} (1,0,1,1,0,1,1,1,0,0,0,1,0,0,0,0)$	5,7,10,12,18	4,6,9,11,13,18	$2^{-17.5}$
$(0,0,0,1,1,1,1,0,1,1,1,1,1,0,0,1) \xrightarrow{1r} (0,1,0,0,1,0,0,0,1,1,1,0,1,1,1,0)$	5,7,10,12,16,17	4,6,9,11,13,17	2^{-12}
$(0,0,0,1,1,1,1,0,1,1,1,1,1,0,1,0) \xrightarrow{1r} (0,1,1,1,0,1,1,0,0,0,0,1,0,0,0,0)$	5,7,10,12	4,6,9,11,13,15	$2^{-17.5}$
$(0,0,0,1,1,1,1,0,1,1,1,1,1,0,1,1) \xrightarrow{1r} (1,0,0,0,1,0,0,1,1,1,1,0,1,1,1,0)$	5,7,10,12,16,17,18	4,6,9,11,13,15,17,18	2^{-12}
$(0,0,0,1,1,1,1,0,1,1,1,1,1,1,0,0) \xrightarrow{1r} (0,1,1,0,1,0,1,0,0,1,1,0,1,1,1,1)$	5,7,10,12,14,17	4,6,9,11,13,17	2^{-12}
$(0,0,0,1,1,1,1,0,1,1,1,1,1,1,0,1) \xrightarrow{1r} (1,0,0,1,0,1,0,1,1,0,0,1,0,0,0,1)$	5,7,10,12,14,16,18	4,6,9,11,13,18	$2^{-28.5}$
$(0,0,0,1,1,1,1,0,1,1,1,1,1,1,1,0) \xrightarrow{1r} (1,0,1,0,1,0,1,1,0,1,1,0,1,1,1,1)$	5,7,10,12,14,17,18	4,6,9,11,13,15,17,18	2^{-12}
$(0,0,0,1,1,1,1,0,1,1,1,1,1,1,1,1) \xrightarrow{1r} (0,1,0,1,0,1,0,0,1,0,0,1,0,0,0,1)$	5,7,10,12,14,16	4,6,9,11,13,15	$2^{-28.5}$

Table 0.249 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	5,7,17,18	4,6,8,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	5,7,16	4,6,8	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	5,7,17	4,6,8,15,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	5,7,16,18	4,6,8,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	5,7,14	4,6,8	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	5,7,14,16,17,18	4,6,8,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	5,7,14,18	4,6,8,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	5,7,14,16,17	4,6,8,15,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	5,7,17	4,6,8,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	5,7,16,18	4,6,8,13,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	5,7,17,18	4,6,8,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	5,7,16	4,6,8,13,15	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	5,7,14,18	4,6,8,13,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	5,7,14,16,17	4,6,8,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	5,7,14	4,6,8,13,15	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	5,7,14,16,17,18	4,6,8,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	5,7,12	4,6,8	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	5,7,12,16,17,18	4,6,8,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	5,7,12,18	4,6,8,15,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	5,7,12,16,17	4,6,8,15,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	5,7,12,14,17,18	4,6,8,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	5,7,12,14,16	4,6,8	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	5,7,12,14,17	4,6,8,15,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	5,7,12,14,16,18	4,6,8,15,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	5,7,12,18	4,6,8,13,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	5,7,12,16,17	4,6,8,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	5,7,12	4,6,8,13,15	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	5,7,12,16,17,18	4,6,8,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	5,7,12,14,17	4,6,8,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	5,7,12,14,16,18	4,6,8,13,18	2^{-1}
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	5,7,12,14,17,18	4,6,8,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	5,7,12,14,16	4,6,8,13,15	2^{-1}

Table 0.250 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	5,7,17	4,6,8,11,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	5,7,16,18	4,6,8,11,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	5,7,17,18	4,6,8,11,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	5,7,16	4,6,8,11,15	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	5,7,14,18	4,6,8,11,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	5,7,14,16,17	4,6,8,11,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	5,7,14	4,6,8,11,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	5,7,14,16,17,18	4,6,8,11,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	5,7,17,18	4,6,8,11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	5,7,16	4,6,8,11,13	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	5,7,17	4,6,8,11,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	5,7,16,18	4,6,8,11,13,15,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	5,7,14	4,6,8,11,13	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	5,7,14,16,17,18	4,6,8,11,13,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	5,7,14,18	4,6,8,11,13,15,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	5,7,14,16,17	4,6,8,11,13,15,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	5,7,12,18	4,6,8,11,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	5,7,12,16,17	4,6,8,11,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	5,7,12	4,6,8,11,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	5,7,12,16,17,18	4,6,8,11,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	5,7,12,14,17	4,6,8,11,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	5,7,12,14,16,18	4,6,8,11,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	5,7,12,14,17,18	4,6,8,11,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	5,7,12,14,16	4,6,8,11,15	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	5,7,12	4,6,8,11,13	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	5,7,12,16,17,18	4,6,8,11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	5,7,12,18	4,6,8,11,13,15,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	5,7,12,16,17	4,6,8,11,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	5,7,12,14,17,18	4,6,8,11,13,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	5,7,12,14,16	4,6,8,11,13	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	5,7,12,14,17	4,6,8,11,13,15,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	5,7,12,14,16,18	4,6,8,11,13,15,18	2^{-12}

Table 0.251 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	5,7,10	4,6,8	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	5,7,10,16,17,18	4,6,8,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	5,7,10,18	4,6,8,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	5,7,10,16,17	4,6,8,15,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	5,7,10,14,17,18	4,6,8,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	5,7,10,14,16	4,6,8	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	5,7,10,14,17	4,6,8,15,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	5,7,10,14,16,18	4,6,8,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	5,7,10,18	4,6,8,13,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	5,7,10,16,17	4,6,8,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	5,7,10	4,6,8,13,15	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	5,7,10,16,17,18	4,6,8,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	5,7,10,14,17	4,6,8,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	5,7,10,14,16,18	4,6,8,13,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	5,7,10,14,17,18	4,6,8,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	5,7,10,14,16	4,6,8,13,15	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	5,7,10,12,17,18	4,6,8,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	5,7,10,12,16	4,6,8	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	5,7,10,12,17	4,6,8,15,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	5,7,10,12,16,18	4,6,8,15,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	5,7,10,12,14	4,6,8	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	5,7,10,12,14,16,17,18	4,6,8,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	5,7,10,12,14,18	4,6,8,15,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	5,7,10,12,14,16,17	4,6,8,15,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	5,7,10,12,17	4,6,8,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	5,7,10,12,16,18	4,6,8,13,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	5,7,10,12,17,18	4,6,8,13,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	5,7,10,12,16	4,6,8,13,15	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	5,7,10,12,14,18	4,6,8,13,18	2^{-34}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	5,7,10,12,14,16,17	4,6,8,13,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	5,7,10,12,14	4,6,8,13,15	2^{-34}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	5,7,10,12,14,16,17,18	4,6,8,13,15,17,18	$2^{-17.5}$

Table 0.252 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	5,7,10,18	4,6,8,11,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	5,7,10,16,17	4,6,8,11,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	5,7,10	4,6,8,11,15	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	5,7,10,16,17,18	4,6,8,11,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	5,7,10,14,17	4,6,8,11,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	5,7,10,14,16,18	4,6,8,11,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	5,7,10,14,17,18	4,6,8,11,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	5,7,10,14,16	4,6,8,11,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	5,7,10	4,6,8,11,13	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	5,7,10,16,17,18	4,6,8,11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	5,7,10,18	4,6,8,11,13,15,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	5,7,10,16,17	4,6,8,11,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	5,7,10,14,17,18	4,6,8,11,13,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	5,7,10,14,16	4,6,8,11,13	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	5,7,10,14,17	4,6,8,11,13,15,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	5,7,10,14,16,18	4,6,8,11,13,15,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	5,7,10,12,17	4,6,8,11,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	5,7,10,12,16,18	4,6,8,11,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	5,7,10,12,17,18	4,6,8,11,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	5,7,10,12,16	4,6,8,11,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	5,7,10,12,14,18	4,6,8,11,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	5,7,10,12,14,16,17	4,6,8,11,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	5,7,10,12,14	4,6,8,11,15	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	5,7,10,12,14,16,17,18	4,6,8,11,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	5,7,10,12,17,18	4,6,8,11,13,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	5,7,10,12,16	4,6,8,11,13	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	5,7,10,12,17	4,6,8,11,13,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	5,7,10,12,16,18	4,6,8,11,13,15,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	5,7,10,12,14	4,6,8,11,13	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	5,7,10,12,14,16,17,18	4,6,8,11,13,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	5,7,10,12,14,18	4,6,8,11,13,15,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	5,7,10,12,14,16,17	4,6,8,11,13,15,17	$2^{-6.5}$

Table 0.253 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0,0,0,1,1,1,1,1,1,0,0,0,0,0,0,0) \xrightarrow{1r} (0,1,1,1,0,0,1,0,1,1,1,1,0,1,0,1)$	5,7,17	4,6,8,9,17	$2^{-17.5}$
$(0,0,0,1,1,1,1,1,1,0,0,0,0,0,0,1) \xrightarrow{1r} (1,0,0,0,1,1,0,1,0,0,0,0,1,0,1,1)$	5,7,16,18	4,6,8,9,18	2^{-12}
$(0,0,0,1,1,1,1,1,1,0,0,0,0,0,1,0) \xrightarrow{1r} (1,0,1,1,0,0,1,1,1,1,1,1,0,1,0,1)$	5,7,17,18	4,6,8,9,15,17,18	$2^{-17.5}$
$(0,0,0,1,1,1,1,1,1,0,0,0,0,0,1,1) \xrightarrow{1r} (0,1,0,0,1,1,0,0,0,0,0,0,1,0,1,1)$	5,7,16	4,6,8,9,15	2^{-12}
$(0,0,0,1,1,1,1,1,1,0,0,0,0,1,0,0) \xrightarrow{1r} (1,0,1,0,1,1,1,1,1,0,0,0,1,0,1,0)$	5,7,14,18	4,6,8,9,18	2^{-23}
$(0,0,0,1,1,1,1,1,1,0,0,0,0,1,0,1) \xrightarrow{1r} (0,1,0,1,0,0,0,0,0,1,1,1,0,1,0,0)$	5,7,14,16,17	4,6,8,9,17	$2^{-17.5}$
$(0,0,0,1,1,1,1,1,1,0,0,0,0,1,1,0) \xrightarrow{1r} (0,1,1,0,1,1,1,0,1,0,0,0,1,0,1,0)$	5,7,14	4,6,8,9,15	2^{-23}
$(0,0,0,1,1,1,1,1,1,0,0,0,0,1,1,1) \xrightarrow{1r} (1,0,0,1,0,0,0,1,0,1,1,1,0,1,0,0)$	5,7,14,16,17,18	4,6,8,9,15,17,18	$2^{-17.5}$
$(0,0,0,1,1,1,1,1,1,0,0,0,0,1,0,0) \xrightarrow{1r} (1,0,1,0,0,1,1,0,1,0,1,1,0,1,0,1)$	5,7,17,18	4,6,8,9,13,17,18	2^{-23}
$(0,0,0,1,1,1,1,1,1,0,0,0,0,1,0,1) \xrightarrow{1r} (0,1,0,1,1,0,0,1,0,1,0,0,1,0,1,1)$	5,7,16	4,6,8,9,13	$2^{-17.5}$
$(0,0,0,1,1,1,1,1,1,0,0,0,0,1,0,1) \xrightarrow{1r} (0,1,1,0,0,1,1,1,1,0,1,1,0,1,0,1)$	5,7,17	4,6,8,9,13,15,17	2^{-23}
$(0,0,0,1,1,1,1,1,1,0,0,0,0,1,0,1) \xrightarrow{1r} (1,0,0,1,1,0,0,0,0,1,0,0,1,0,1,1)$	5,7,16,18	4,6,8,9,13,15,18	$2^{-17.5}$
$(0,0,0,1,1,1,1,1,1,0,0,0,0,1,1,0) \xrightarrow{1r} (0,1,1,1,1,0,1,1,1,1,0,0,1,0,1,0)$	5,7,14	4,6,8,9,13	$2^{-17.5}$
$(0,0,0,1,1,1,1,1,1,0,0,0,0,1,1,0) \xrightarrow{1r} (1,0,0,0,0,1,0,0,0,0,1,1,0,1,0,0)$	5,7,14,16,17,18	4,6,8,9,13,17,18	2^{-12}
$(0,0,0,1,1,1,1,1,1,0,0,0,0,1,1,1) \xrightarrow{1r} (1,0,1,1,1,0,1,0,1,1,0,0,1,0,1,0)$	5,7,14,18	4,6,8,9,13,15,18	$2^{-17.5}$
$(0,0,0,1,1,1,1,1,1,0,0,0,0,1,1,1) \xrightarrow{1r} (0,1,0,0,0,1,0,1,0,0,1,1,0,1,0,0)$	5,7,14,16,17	4,6,8,9,13,15,17	2^{-12}
$(0,0,0,1,1,1,1,1,1,0,0,0,0,1,0,0) \xrightarrow{1r} (1,0,1,0,1,1,0,1,1,0,1,0,1,0,1,0)$	5,7,12,18	4,6,8,9,18	2^{-23}
$(0,0,0,1,1,1,1,1,1,0,0,0,1,0,0,0) \xrightarrow{1r} (0,1,0,1,0,0,1,0,0,1,0,1,0,1,0,0)$	5,7,12,16,17	4,6,8,9,17	$2^{-28.5}$
$(0,0,0,1,1,1,1,1,1,0,0,0,1,0,0,1) \xrightarrow{1r} (0,1,1,0,1,1,0,0,1,0,1,0,1,0,1,0)$	5,7,12	4,6,8,9,15	2^{-23}
$(0,0,0,1,1,1,1,1,1,0,0,0,1,0,0,1) \xrightarrow{1r} (1,0,0,1,0,0,1,1,0,1,0,1,0,1,0,0)$	5,7,12,16,17,18	4,6,8,9,15,17,18	$2^{-28.5}$
$(0,0,0,1,1,1,1,1,1,0,0,0,1,0,1,0) \xrightarrow{1r} (0,1,1,1,0,0,0,0,1,1,0,1,0,1,0,1)$	5,7,12,14,17	4,6,8,9,17	$2^{-28.5}$
$(0,0,0,1,1,1,1,1,1,0,0,0,1,0,1,0) \xrightarrow{1r} (1,0,0,0,1,1,1,1,0,0,1,0,1,0,1,1)$	5,7,12,14,16,18	4,6,8,9,18	2^{-12}
$(0,0,0,1,1,1,1,1,1,0,0,0,1,0,1,1) \xrightarrow{1r} (1,0,1,1,0,0,0,1,1,1,0,1,0,1,0,1)$	5,7,12,14,17,18	4,6,8,9,15,17,18	$2^{-28.5}$
$(0,0,0,1,1,1,1,1,1,0,0,0,1,0,1,1) \xrightarrow{1r} (0,1,0,0,1,1,1,0,0,0,1,0,1,0,1,1)$	5,7,12,14,16	4,6,8,9,15	2^{-12}
$(0,0,0,1,1,1,1,1,1,0,0,0,1,1,0,0) \xrightarrow{1r} (0,1,1,1,1,0,0,1,1,1,1,0,1,0,1,0)$	5,7,12	4,6,8,9,13	$2^{-17.5}$
$(0,0,0,1,1,1,1,1,1,0,0,0,1,1,0,0) \xrightarrow{1r} (1,0,0,0,0,1,1,0,0,0,0,1,0,1,0,0)$	5,7,12,16,17,18	4,6,8,9,13,17,18	2^{-23}
$(0,0,0,1,1,1,1,1,1,0,0,0,1,1,0,1) \xrightarrow{1r} (1,0,1,1,1,0,0,0,1,1,1,0,1,0,1,0)$	5,7,12,18	4,6,8,9,13,15,18	$2^{-17.5}$
$(0,0,0,1,1,1,1,1,1,0,0,0,1,1,0,1) \xrightarrow{1r} (0,1,0,0,0,1,1,1,0,0,0,1,0,1,0,0)$	5,7,12,16,17	4,6,8,9,13,15,17	2^{-23}
$(0,0,0,1,1,1,1,1,1,0,0,0,1,1,1,0) \xrightarrow{1r} (1,0,1,0,0,1,0,0,1,0,0,1,0,1,0,1)$	5,7,12,14,17,18	4,6,8,9,13,17,18	2^{-34}
$(0,0,0,1,1,1,1,1,1,0,0,0,1,1,1,0) \xrightarrow{1r} (0,1,0,1,1,0,1,1,0,1,1,0,1,0,1,1)$	5,7,12,14,16	4,6,8,9,13	$2^{-17.5}$
$(0,0,0,1,1,1,1,1,1,0,0,0,1,1,1,1) \xrightarrow{1r} (0,1,1,0,0,1,0,1,1,0,0,1,0,1,0,1)$	5,7,12,14,17	4,6,8,9,13,15,17	2^{-34}
$(0,0,0,1,1,1,1,1,1,0,0,0,1,1,1,1) \xrightarrow{1r} (1,0,0,1,1,0,1,0,0,1,1,0,1,0,1,1)$	5,7,12,14,16,18	4,6,8,9,13,15,18	$2^{-17.5}$

Table 0.254 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	5,7,17,18	4,6,8,9,11,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	5,7,16	4,6,8,9,11	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	5,7,17	4,6,8,9,11,15,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	5,7,16,18	4,6,8,9,11,15,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	5,7,14	4,6,8,9,11	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	5,7,14,16,17,18	4,6,8,9,11,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	5,7,14,18	4,6,8,9,11,15,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	5,7,14,16,17	4,6,8,9,11,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	5,7,17	4,6,8,9,11,13,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	5,7,16,18	4,6,8,9,11,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	5,7,17,18	4,6,8,9,11,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	5,7,16	4,6,8,9,11,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	5,7,14,18	4,6,8,9,11,13,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	5,7,14,16,17	4,6,8,9,11,13,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	5,7,14	4,6,8,9,11,13,15	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	5,7,14,16,17,18	4,6,8,9,11,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	5,7,12	4,6,8,9,11	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	5,7,12,16,17,18	4,6,8,9,11,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	5,7,12,18	4,6,8,9,11,15,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	5,7,12,16,17	4,6,8,9,11,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	5,7,12,14,17,18	4,6,8,9,11,17,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	5,7,12,14,16	4,6,8,9,11	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	5,7,12,14,17	4,6,8,9,11,15,17	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	5,7,12,14,16,18	4,6,8,9,11,15,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	5,7,12,18	4,6,8,9,11,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	5,7,12,16,17	4,6,8,9,11,13,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	5,7,12	4,6,8,9,11,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	5,7,12,16,17,18	4,6,8,9,11,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	5,7,12,14,17	4,6,8,9,11,13,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	5,7,12,14,16,18	4,6,8,9,11,13,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	5,7,12,14,17,18	4,6,8,9,11,13,15,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	5,7,12,14,16	4,6,8,9,11,13,15	$2^{-6.5}$

Table 0.255 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	5,7,10,18	4,6,8,9,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	5,7,10,16,17	4,6,8,9,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	5,7,10	4,6,8,9,15	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	5,7,10,16,17,18	4,6,8,9,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	5,7,10,14,17	4,6,8,9,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	5,7,10,14,16,18	4,6,8,9,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	5,7,10,14,17,18	4,6,8,9,15,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	5,7,10,14,16	4,6,8,9,15	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	5,7,10	4,6,8,9,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	5,7,10,16,17,18	4,6,8,9,13,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	5,7,10,18	4,6,8,9,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	5,7,10,16,17	4,6,8,9,13,15,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	5,7,10,14,17,18	4,6,8,9,13,17,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	5,7,10,14,16	4,6,8,9,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	5,7,10,14,17	4,6,8,9,13,15,17	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	5,7,10,14,16,18	4,6,8,9,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	5,7,10,12,17	4,6,8,9,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	5,7,10,12,16,18	4,6,8,9,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	5,7,10,12,17,18	4,6,8,9,15,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	5,7,10,12,16	4,6,8,9,15	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	5,7,10,12,14,18	4,6,8,9,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	5,7,10,12,14,16,17	4,6,8,9,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	5,7,10,12,14	4,6,8,9,15	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	5,7,10,12,14,16,17,18	4,6,8,9,15,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	5,7,10,12,17,18	4,6,8,9,13,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	5,7,10,12,16	4,6,8,9,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	5,7,10,12,17	4,6,8,9,13,15,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	5,7,10,12,16,18	4,6,8,9,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	5,7,10,12,14	4,6,8,9,13	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	5,7,10,12,14,16,17,18	4,6,8,9,13,17,18	2^{-1}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	5,7,10,12,14,18	4,6,8,9,13,15,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	5,7,10,12,14,16,17	4,6,8,9,13,15,17	2^{-1}

Table 0.256 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	5,7,10	4,6,8,9,11	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	5,7,10,16,17,18	4,6,8,9,11,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	5,7,10,18	4,6,8,9,11,15,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	5,7,10,16,17	4,6,8,9,11,15,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	5,7,10,14,17,18	4,6,8,9,11,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	5,7,10,14,16	4,6,8,9,11	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	5,7,10,14,17	4,6,8,9,11,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	5,7,10,14,16,18	4,6,8,9,11,15,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	5,7,10,18	4,6,8,9,11,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	5,7,10,16,17	4,6,8,9,11,13,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	5,7,10	4,6,8,9,11,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	5,7,10,16,17,18	4,6,8,9,11,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	5,7,10,14,17	4,6,8,9,11,13,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	5,7,10,14,16,18	4,6,8,9,11,13,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	5,7,10,14,17,18	4,6,8,9,11,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	5,7,10,14,16	4,6,8,9,11,13,15	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	5,7,10,12,17,18	4,6,8,9,11,17,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	5,7,10,12,16	4,6,8,9,11	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	5,7,10,12,17	4,6,8,9,11,15,17	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	5,7,10,12,16,18	4,6,8,9,11,15,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	5,7,10,12,14	4,6,8,9,11	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	5,7,10,12,14,16,17,18	4,6,8,9,11,17,18	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	5,7,10,12,14,18	4,6,8,9,11,15,18	2^{-23}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	5,7,10,12,14,16,17	4,6,8,9,11,15,17	$2^{-6.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	5,7,10,12,17	4,6,8,9,11,13,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	5,7,10,12,16,18	4,6,8,9,11,13,18	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	5,7,10,12,17,18	4,6,8,9,11,13,15,17,18	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	5,7,10,12,16	4,6,8,9,11,13,15	$2^{-17.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	5,7,10,12,14,18	4,6,8,9,11,13,18	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	5,7,10,12,14,16,17	4,6,8,9,11,13,17	2^{-12}
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	5,7,10,12,14	4,6,8,9,11,13,15	$2^{-28.5}$
$(0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	5,7,10,12,14,16,17,18	4,6,8,9,11,13,15,17,18	2^{-12}

Table 0.257 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	3,18	18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	3,16,17	17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	3	15	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	3,16,17,18	15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	3,14,17	17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	3,14,16,18	18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	3,14,17,18	15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	3,14,16	15	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	3	13	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	3,16,17,18	13,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	3,18	13,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	3,16,17	13,15,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	3,14,17,18	13,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	3,14,16	13	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	3,14,17	13,15,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	3,14,16,18	13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	3,12,17	17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,12,16,18	18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	3,12,17,18	15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	3,12,16	15	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	3,12,14,18	18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	3,12,14,16,17	17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	3,12,14	15	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	3,12,14,16,17,18	15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	3,12,17,18	13,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	3,12,16	13	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	3,12,17	13,15,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	3,12,16,18	13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	3,12,14	13	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	3,12,14,16,17,18	13,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	3,12,14,18	13,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	3,12,14,16,17	13,15,17	2^{-12}

Table 0.258 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	3	11	2^{-1}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	3,16,17,18	11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	3,18	11,15,18	2^{-1}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	3,16,17	11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	3,14,17,18	11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	3,14,16	11	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	3,14,17	11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	3,14,16,18	11,15,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	3,18	11,13,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	3,16,17	11,13,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	3	11,13,15	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	3,16,17,18	11,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	3,14,17	11,13,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	3,14,16,18	11,13,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	3,14,17,18	11,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	3,14,16	11,13,15	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	3,12,17,18	11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	3,12,16	11	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	3,12,17	11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	3,12,16,18	11,15,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	3,12,14	11	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	3,12,14,16,17,18	11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	3,12,14,18	11,15,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	3,12,14,16,17	11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	3,12,17	11,13,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	3,12,16,18	11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	3,12,17,18	11,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	3,12,16	11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	3,12,14,18	11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	3,12,14,16,17	11,13,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	3,12,14	11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	3,12,14,16,17,18	11,13,15,17,18	2^{-23}

Table 0.259 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,10,17	17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	3,10,16,18	18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	3,10,17,18	15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	3,10,16	15	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	3,10,14,18	18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	3,10,14,16,17	17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	3,10,14	15	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	3,10,14,16,17,18	15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,10,17,18	13,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,10,16	13	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,10,17	13,15,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	3,10,16,18	13,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	3,10,14	13	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	3,10,14,16,17,18	13,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	3,10,14,18	13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	3,10,14,16,17	13,15,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	3,10,12,18	18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	3,10,12,16,17	17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	3,10,12	15	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	3,10,12,16,17,18	15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	3,10,12,14,17	17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	3,10,12,14,16,18	18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	3,10,12,14,17,18	15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	3,10,12,14,16	15	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	3,10,12	13	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	3,10,12,16,17,18	13,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	3,10,12,18	13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	3,10,12,16,17	13,15,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	3,10,12,14,17,18	13,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	3,10,12,14,16	13	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	3,10,12,14,17	13,15,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	3,10,12,14,16,18	13,15,18	$2^{-28.5}$

Table 0.260 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	3,10,17,18	11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	3,10,16	11	2^{-34}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	3,10,17	11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	3,10,16,18	11,15,18	2^{-34}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	3,10,14	11	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	3,10,14,16,17,18	11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	3,10,14,18	11,15,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	3,10,14,16,17	11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	3,10,17	11,13,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	3,10,16,18	11,13,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	3,10,17,18	11,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	3,10,16	11,13,15	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	3,10,14,18	11,13,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	3,10,14,16,17	11,13,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	3,10,14	11,13,15	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	3,10,14,16,17,18	11,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	3,10,12	11	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	3,10,12,16,17,18	11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	3,10,12,18	11,15,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	3,10,12,16,17	11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	3,10,12,14,17,18	11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	3,10,12,14,16	11	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	3,10,12,14,17	11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	3,10,12,14,16,18	11,15,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	3,10,12,18	11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	3,10,12,16,17	11,13,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	3,10,12	11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	3,10,12,16,17,18	11,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	3,10,12,14,17	11,13,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	3,10,12,14,16,18	11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	3,10,12,14,17,18	11,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	3,10,12,14,16	11,13,15	$2^{-17.5}$

Table 0.261 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	3	9	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	3,16,17,18	9,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	3,18	9,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	3,16,17	9,15,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	3,14,17,18	9,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	3,14,16	9	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	3,14,17	9,15,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	3,14,16,18	9,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	3,18	9,13,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	3,16,17	9,13,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	3	9,13,15	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	3,16,17,18	9,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	3,14,17	9,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	3,14,16,18	9,13,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	3,14,17,18	9,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	3,14,16	9,13,15	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	3,12,17,18	9,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	3,12,16	9	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	3,12,17	9,15,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	3,12,16,18	9,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	3,12,14	9	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	3,12,14,16,17,18	9,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	3,12,14,18	9,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	3,12,14,16,17	9,15,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	3,12,17	9,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	3,12,16,18	9,13,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	3,12,17,18	9,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	3,12,16	9,13,15	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	3,12,14,18	9,13,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	3,12,14,16,17	9,13,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	3,12,14	9,13,15	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	3,12,14,16,17,18	9,13,15,17,18	$2^{-28.5}$

Table 0.262 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	3,18	9,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	3,16,17	9,11,17	2^{-34}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	3	9,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	3,16,17,18	9,11,15,17,18	2^{-34}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	3,14,17	9,11,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	3,14,16,18	9,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	3,14,17,18	9,11,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	3,14,16	9,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	3	9,11,13	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,16,17,18	9,11,13,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	3,18	9,11,13,15,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	3,16,17	9,11,13,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	3,14,17,18	9,11,13,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	3,14,16	9,11,13	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	3,14,17	9,11,13,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	3,14,16,18	9,11,13,15,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	3,12,17	9,11,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	3,12,16,18	9,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	3,12,17,18	9,11,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	3,12,16	9,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	3,12,14,18	9,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	3,12,14,16,17	9,11,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	3,12,14	9,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	3,12,14,16,17,18	9,11,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	3,12,17,18	9,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	3,12,16	9,11,13	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	3,12,17	9,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	3,12,16,18	9,11,13,15,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	3,12,14	9,11,13	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	3,12,14,16,17,18	9,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	3,12,14,18	9,11,13,15,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	3,12,14,16,17	9,11,13,15,17	$2^{-17.5}$

Table 0.263 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	3,10,17,18	9,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	3,10,16	9	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	3,10,17	9,15,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	3,10,16,18	9,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	3,10,14	9	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	3,10,14,16,17,18	9,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	3,10,14,18	9,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	3,10,14,16,17	9,15,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	3,10,17	9,13,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	3,10,16,18	9,13,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	3,10,17,18	9,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	3,10,16	9,13,15	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	3,10,14,18	9,13,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	3,10,14,16,17	9,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	3,10,14	9,13,15	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	3,10,14,16,17,18	9,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	3,10,12	9	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	3,10,12,16,17,18	9,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	3,10,12,18	9,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	3,10,12,16,17	9,15,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	3,10,12,14,17,18	9,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	3,10,12,14,16	9	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	3,10,12,14,17	9,15,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	3,10,12,14,16,18	9,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	3,10,12,18	9,13,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	3,10,12,16,17	9,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	3,10,12	9,13,15	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	3,10,12,16,17,18	9,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	3,10,12,14,17	9,13,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	3,10,12,14,16,18	9,13,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	3,10,12,14,17,18	9,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	3,10,12,14,16	9,13,15	2^{-12}

Table 0.264 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	3,10,17	9,11,17	2^{-1}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	3,10,16,18	9,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	3,10,17,18	9,11,15,17,18	2^{-1}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	3,10,16	9,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	3,10,14,18	9,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	3,10,14,16,17	9,11,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	3,10,14	9,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	3,10,14,16,17,18	9,11,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,10,17,18	9,11,13,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	3,10,16	9,11,13	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	3,10,17	9,11,13,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	3,10,16,18	9,11,13,15,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	3,10,14	9,11,13	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	3,10,14,16,17,18	9,11,13,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	3,10,14,18	9,11,13,15,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	3,10,14,16,17	9,11,13,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	3,10,12,18	9,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	3,10,12,16,17	9,11,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	3,10,12	9,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	3,10,12,16,17,18	9,11,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	3,10,12,14,17	9,11,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	3,10,12,14,16,18	9,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	3,10,12,14,17,18	9,11,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	3,10,12,14,16	9,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	3,10,12	9,11,13	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	3,10,12,16,17,18	9,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	3,10,12,18	9,11,13,15,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	3,10,12,16,17	9,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	3,10,12,14,17,18	9,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	3,10,12,14,16	9,11,13	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	3,10,12,14,17	9,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	3,10,12,14,16,18	9,11,13,15,18	2^{-23}

Table 0.265 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	3,17	8,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	3,16,18	8,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	3,17,18	8,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	3,16	8,15	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	3,14,18	8,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	3,14,16,17	8,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	3,14	8,15	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	3,14,16,17,18	8,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	3,17,18	8,13,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	3,16	8,13	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	3,17	8,13,15,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	3,16,18	8,13,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	3,14	8,13	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	3,14,16,17,18	8,13,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	3,14,18	8,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	3,14,16,17	8,13,15,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	3,12,18	8,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	3,12,16,17	8,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	3,12	8,15	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	3,12,16,17,18	8,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	3,12,14,17	8,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	3,12,14,16,18	8,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	3,12,14,17,18	8,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	3,12,14,16	8,15	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	3,12	8,13	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	3,12,16,17,18	8,13,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	3,12,18	8,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	3,12,16,17	8,13,15,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	3,12,14,17,18	8,13,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	3,12,14,16	8,13	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	3,12,14,17	8,13,15,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	3,12,14,16,18	8,13,15,18	$2^{-6.5}$

Table 0.266 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	3,17,18	8,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	3,16	8,11	2^{-1}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	3,17	8,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	3,16,18	8,11,15,18	2^{-1}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	3,14	8,11	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	3,14,16,17,18	8,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	3,14,18	8,11,15,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	3,14,16,17	8,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	3,17	8,11,13,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,16,18	8,11,13,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	3,17,18	8,11,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	3,16	8,11,13,15	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	3,14,18	8,11,13,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	3,14,16,17	8,11,13,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	3,14	8,11,13,15	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	3,14,16,17,18	8,11,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	3,12	8,11	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	3,12,16,17,18	8,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	3,12,18	8,11,15,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	3,12,16,17	8,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	3,12,14,17,18	8,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	3,12,14,16	8,11	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	3,12,14,17	8,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	3,12,14,16,18	8,11,15,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	3,12,18	8,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	3,12,16,17	8,11,13,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	3,12	8,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	3,12,16,17,18	8,11,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	3,12,14,17	8,11,13,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	3,12,14,16,18	8,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	3,12,14,17,18	8,11,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	3,12,14,16	8,11,13,15	$2^{-17.5}$

Table 0.267 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	3,10,18	8,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	3,10,16,17	8,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	3,10	8,15	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	3,10,16,17,18	8,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	3,10,14,17	8,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	3,10,14,16,18	8,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	3,10,14,17,18	8,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	3,10,14,16	8,15	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	3,10	8,13	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	3,10,16,17,18	8,13,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	3,10,18	8,13,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	3,10,16,17	8,13,15,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	3,10,14,17,18	8,13,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	3,10,14,16	8,13	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	3,10,14,17	8,13,15,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	3,10,14,16,18	8,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	3,10,12,17	8,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	3,10,12,16,18	8,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	3,10,12,17,18	8,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	3,10,12,16	8,15	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	3,10,12,14,18	8,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	3,10,12,14,16,17	8,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	3,10,12,14	8,15	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	3,10,12,14,16,17,18	8,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	3,10,12,17,18	8,13,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	3,10,12,16	8,13	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	3,10,12,17	8,13,15,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	3,10,12,16,18	8,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	3,10,12,14	8,13	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	3,10,12,14,16,17,18	8,13,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	3,10,12,14,18	8,13,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	3,10,12,14,16,17	8,13,15,17	2^{-23}

Table 0.268 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	3,10	8,11	2^{-34}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	3,10,16,17,18	8,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	3,10,18	8,11,15,18	2^{-34}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	3,10,16,17	8,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	3,10,14,17,18	8,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	3,10,14,16	8,11	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	3,10,14,17	8,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	3,10,14,16,18	8,11,15,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,10,18	8,11,13,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	3,10,16,17	8,11,13,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	3,10	8,11,13,15	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	3,10,16,17,18	8,11,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	3,10,14,17	8,11,13,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	3,10,14,16,18	8,11,13,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	3,10,14,17,18	8,11,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	3,10,14,16	8,11,13,15	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	3,10,12,17,18	8,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	3,10,12,16	8,11	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	3,10,12,17	8,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	3,10,12,16,18	8,11,15,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	3,10,12,14	8,11	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	3,10,12,14,16,17,18	8,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	3,10,12,14,18	8,11,15,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	3,10,12,14,16,17	8,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	3,10,12,17	8,11,13,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	3,10,12,16,18	8,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	3,10,12,17,18	8,11,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	3,10,12,16	8,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	3,10,12,14,18	8,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	3,10,12,14,16,17	8,11,13,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	3,10,12,14	8,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	3,10,12,14,16,17,18	8,11,13,15,17,18	2^{-12}

Table 0.269 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	3,17,18	8,9,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,16	8,9	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	3,17	8,9,15,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	3,16,18	8,9,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	3,14	8,9	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	3,14,16,17,18	8,9,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	3,14,18	8,9,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	3,14,16,17	8,9,15,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,17	8,9,13,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,16,18	8,9,13,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	3,17,18	8,9,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	3,16	8,9,13,15	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	3,14,18	8,9,13,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	3,14,16,17	8,9,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	3,14	8,9,13,15	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	3,14,16,17,18	8,9,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	3,12	8,9	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	3,12,16,17,18	8,9,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	3,12,18	8,9,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	3,12,16,17	8,9,15,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	3,12,14,17,18	8,9,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	3,12,14,16	8,9	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	3,12,14,17	8,9,15,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	3,12,14,16,18	8,9,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	3,12,18	8,9,13,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	3,12,16,17	8,9,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	3,12	8,9,13,15	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	3,12,16,17,18	8,9,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	3,12,14,17	8,9,13,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	3,12,14,16,18	8,9,13,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	3,12,14,17,18	8,9,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	3,12,14,16	8,9,13,15	2^{-23}

Table 0.270 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	3,17	8,9,11,17	2^{-34}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	3,16,18	8,9,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	3,17,18	8,9,11,15,17,18	2^{-34}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	3,16	8,9,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	3,14,18	8,9,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	3,14,16,17	8,9,11,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	3,14	8,9,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	3,14,16,17,18	8,9,11,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	3,17,18	8,9,11,13,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	3,16	8,9,11,13	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	3,17	8,9,11,13,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	3,16,18	8,9,11,13,15,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	3,14	8,9,11,13	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	3,14,16,17,18	8,9,11,13,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	3,14,18	8,9,11,13,15,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	3,14,16,17	8,9,11,13,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	3,12,18	8,9,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	3,12,16,17	8,9,11,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	3,12	8,9,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	3,12,16,17,18	8,9,11,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	3,12,14,17	8,9,11,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	3,12,14,16,18	8,9,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	3,12,14,17,18	8,9,11,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	3,12,14,16	8,9,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	3,12	8,9,11,13	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	3,12,16,17,18	8,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	3,12,18	8,9,11,13,15,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	3,12,16,17	8,9,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	3,12,14,17,18	8,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	3,12,14,16	8,9,11,13	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	3,12,14,17	8,9,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	3,12,14,16,18	8,9,11,13,15,18	2^{-12}

Table 0.271 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	3,10	8,9	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	3,10,16,17,18	8,9,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	3,10,18	8,9,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	3,10,16,17	8,9,15,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	3,10,14,17,18	8,9,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	3,10,14,16	8,9	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	3,10,14,17	8,9,15,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	3,10,14,16,18	8,9,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	3,10,18	8,9,13,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	3,10,16,17	8,9,13,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	3,10	8,9,13,15	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	3,10,16,17,18	8,9,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	3,10,14,17	8,9,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	3,10,14,16,18	8,9,13,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	3,10,14,17,18	8,9,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	3,10,14,16	8,9,13,15	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,10,12,17,18	8,9,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	3,10,12,16	8,9	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	3,10,12,17	8,9,15,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	3,10,12,16,18	8,9,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	3,10,12,14	8,9	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	3,10,12,14,16,17,18	8,9,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	3,10,12,14,18	8,9,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	3,10,12,14,16,17	8,9,15,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	3,10,12,17	8,9,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	3,10,12,16,18	8,9,13,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	3,10,12,17,18	8,9,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	3,10,12,16	8,9,13,15	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	3,10,12,14,18	8,9,13,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	3,10,12,14,16,17	8,9,13,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	3,10,12,14	8,9,13,15	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	3,10,12,14,16,17,18	8,9,13,15,17,18	$2^{-6.5}$

Table 0.272 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	3,10,18	8,9,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	3,10,16,17	8,9,11,17	2^{-1}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	3,10	8,9,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	3,10,16,17,18	8,9,11,15,17,18	2^{-1}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	3,10,14,17	8,9,11,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	3,10,14,16,18	8,9,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	3,10,14,17,18	8,9,11,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	3,10,14,16	8,9,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	3,10	8,9,11,13	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	3,10,16,17,18	8,9,11,13,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	3,10,18	8,9,11,13,15,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	3,10,16,17	8,9,11,13,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	3,10,14,17,18	8,9,11,13,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	3,10,14,16	8,9,11,13	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	3,10,14,17	8,9,11,13,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	3,10,14,16,18	8,9,11,13,15,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	3,10,12,17	8,9,11,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	3,10,12,16,18	8,9,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	3,10,12,17,18	8,9,11,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	3,10,12,16	8,9,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	3,10,12,14,18	8,9,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	3,10,12,17,18	8,9,11,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	3,10,12,14	8,9,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	3,10,12,14,16,17,18	8,9,11,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	3,10,12,17,18	8,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	3,10,12,16	8,9,11,13	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	3,10,12,17	8,9,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	3,10,12,16,18	8,9,11,13,15,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	3,10,12,14	8,9,11,13	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	3,10,12,14,16,17,18	8,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	3,10,12,14,18	8,9,11,13,15,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	3,10,12,14,16,17	8,9,11,13,15,17	$2^{-17.5}$

Table 0.273 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	3,7	—	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	3,7,16,17,18	17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	3,7,18	15,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	3,7,16,17	15,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	3,7,14,17,18	17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	3,7,14,16	—	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	3,7,14,17	15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	3,7,14,16,18	15,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	3,7,18	13,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	3,7,16,17	13,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	3,7	13,15	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,7,16,17,18	13,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	3,7,14,17	13,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	3,7,14,16,18	13,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	3,7,14,17,18	13,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	3,7,14,16	13,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	3,7,12,17,18	17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	3,7,12,16	—	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	3,7,12,17	15,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	3,7,12,16,18	15,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	3,7,12,14	—	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	3,7,12,14,16,17,18	17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	3,7,12,14,18	15,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	3,7,12,14,16,17	15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	3,7,12,17	13,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	3,7,12,16,18	13,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	3,7,12,17,18	13,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	3,7,12,16	13,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	3,7,12,14,18	13,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	3,7,12,14,16,17	13,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	3,7,12,14	13,15	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	3,7,12,14,16,17,18	13,15,17,18	2^{-12}

Table 0.274 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	3,7,18	11,18	2^{-1}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	3,7,16,17	11,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	3,7	11,15	2^{-1}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	3,7,16,17,18	11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	3,7,14,17	11,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	3,7,14,16,18	11,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	3,7,14,17,18	11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	3,7,14,16	11,15	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	3,7	11,13	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	3,7,16,17,18	11,13,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	3,7,18	11,13,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	3,7,16,17	11,13,15,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	3,7,14,17,18	11,13,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	3,7,14,16	11,13	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	3,7,14,17	11,13,15,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	3,7,14,16,18	11,13,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	3,7,12,17	11,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	3,7,12,16,18	11,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	3,7,12,17,18	11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	3,7,12,16	11,15	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	3,7,12,14,18	11,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	3,7,12,14,16,17	11,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	3,7,12,14	11,15	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	3,7,12,14,16,17,18	11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	3,7,12,17,18	11,13,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	3,7,12,16	11,13	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	3,7,12,17	11,13,15,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	3,7,12,16,18	11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	3,7,12,14	11,13	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	3,7,12,14,16,17,18	11,13,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	3,7,12,14,18	11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	3,7,12,14,16,17	11,13,15,17	2^{-23}

Table 0.275 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	3,7,10,17,18	17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	3,7,10,16	—	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	3,7,10,17	15,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	3,7,10,16,18	15,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	3,7,10,14	—	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	3,7,10,14,16,17,18	17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	3,7,10,14,18	15,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	3,7,10,14,16,17	15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	3,7,10,17	13,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	3,7,10,16,18	13,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,7,10,17,18	13,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	3,7,10,16	13,15	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	3,7,10,14,18	13,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	3,7,10,14,16,17	13,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	3,7,10,14	13,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	3,7,10,14,16,17,18	13,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	3,7,10,12	—	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,7,10,12,16,17,18	17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	3,7,10,12,18	15,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	3,7,10,12,16,17	15,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	3,7,10,12,14,17,18	17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	3,7,10,12,14,16	—	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	3,7,10,12,14,17	15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	3,7,10,12,14,16,18	15,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	3,7,10,12,18	13,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	3,7,10,12,16,17	13,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	3,7,10,12	13,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	3,7,10,12,16,17,18	13,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	3,7,10,12,14,17	13,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	3,7,10,12,14,16,18	13,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	3,7,10,12,14,17,18	13,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	3,7,10,12,14,16	13,15	$2^{-28.5}$

Table 0.276 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	3,7,10,17	11,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	3,7,10,16,18	11,18	2^{-34}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	3,7,10,17,18	11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	3,7,10,16	11,15	2^{-34}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	3,7,10,14,18	11,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	3,7,10,14,16,17	11,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	3,7,10,14	11,15	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	3,7,10,14,16,17,18	11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	3,7,10,17,18	11,13,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	3,7,10,16	11,13	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	3,7,10,17	11,13,15,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	3,7,10,16,18	11,13,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	3,7,10,14	11,13	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	3,7,10,14,16,17,18	11,13,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	3,7,10,14,18	11,13,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	3,7,10,14,16,17	11,13,15,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	3,7,10,12,18	11,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	3,7,10,12,16,17	11,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	3,7,10,12	11,15	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	3,7,10,12,16,17,18	11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	3,7,10,12,14,17	11,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	3,7,10,12,14,16,18	11,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	3,7,10,12,14,17,18	11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	3,7,10,12,14,16	11,15	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	3,7,10,12	11,13	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	3,7,10,12,16,17,18	11,13,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	3,7,10,12,18	11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	3,7,10,12,16,17	11,13,15,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	3,7,10,12,14,17,18	11,13,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	3,7,10,12,14,16	11,13	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	3,7,10,12,14,17	11,13,15,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	3,7,10,12,14,16,18	11,13,15,18	$2^{-17.5}$

Table 0.277 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	3,7,18	9,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	3,7,16,17	9,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	3,7	9,15	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	3,7,16,17,18	9,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	3,7,14,17	9,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	3,7,14,16,18	9,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	3,7,14,17,18	9,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	3,7,14,16	9,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	3,7	9,13	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	3,7,16,17,18	9,13,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	3,7,18	9,13,15,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	3,7,16,17	9,13,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	3,7,14,17,18	9,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	3,7,14,16	9,13	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	3,7,14,17	9,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	3,7,14,16,18	9,13,15,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	3,7,12,17	9,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	3,7,12,16,18	9,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	3,7,12,17,18	9,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	3,7,12,16	9,15	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	3,7,12,14,18	9,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	3,7,12,14,16,17	9,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	3,7,12,14	9,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	3,7,12,14,16,17,18	9,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	3,7,12,17,18	9,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	3,7,12,16	9,13	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	3,7,12,17	9,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	3,7,12,16,18	9,13,15,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	3,7,12,14	9,13	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	3,7,12,14,16,17,18	9,13,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	3,7,12,14,18	9,13,15,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	3,7,12,14,16,17	9,13,15,17	$2^{-28.5}$

Table 0.278 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	3,7	9,11	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	3,7,16,17,18	9,11,17,18	2^{-34}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	3,7,18	9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	3,7,16,17	9,11,15,17	2^{-34}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	3,7,14,17,18	9,11,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	3,7,14,16	9,11	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	3,7,14,17	9,11,15,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	3,7,14,16,18	9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	3,7,18	9,11,13,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	3,7,16,17	9,11,13,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	3,7	9,11,13,15	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	3,7,16,17,18	9,11,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	3,7,14,17	9,11,13,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	3,7,14,16,18	9,11,13,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	3,7,14,17,18	9,11,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	3,7,14,16	9,11,13,15	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	3,7,12,17,18	9,11,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	3,7,12,16	9,11	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	3,7,12,17	9,11,15,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,7,12,16,18	9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	3,7,12,14	9,11	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	3,7,12,14,16,17,18	9,11,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	3,7,12,14,18	9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	3,7,12,14,16,17	9,11,15,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	3,7,12,17	9,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	3,7,12,16,18	9,11,13,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	3,7,12,17,18	9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	3,7,12,16	9,11,13,15	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	3,7,12,14,18	9,11,13,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	3,7,12,14,16,17	9,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	3,7,12,14	9,11,13,15	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	3,7,12,14,16,17,18	9,11,13,15,17,18	$2^{-17.5}$

Table 0.279 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	3,7,10,17	9,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	3,7,10,16,18	9,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	3,7,10,17,18	9,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	3,7,10,16	9,15	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	3,7,10,14,18	9,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	3,7,10,14,16,17	9,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	3,7,10,14	9,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	3,7,10,14,16,17,18	9,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	3,7,10,17,18	9,13,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	3,7,10,16	9,13	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	3,7,10,17	9,13,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	3,7,10,16,18	9,13,15,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	3,7,10,14	9,13	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	3,7,10,14,16,17,18	9,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	3,7,10,14,18	9,13,15,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	3,7,10,14,16,17	9,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	3,7,10,12,18	9,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	3,7,10,12,16,17	9,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	3,7,10,12	9,15	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	3,7,10,12,16,17,18	9,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	3,7,10,12,14,17	9,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	3,7,10,12,14,16,18	9,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	3,7,10,12,14,17,18	9,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	3,7,10,12,14,16	9,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	3,7,10,12	9,13	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	3,7,10,12,16,17,18	9,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	3,7,10,12,18	9,13,15,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	3,7,10,12,16,17	9,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	3,7,10,12,14,17,18	9,13,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	3,7,10,12,14,16	9,13	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	3,7,10,12,14,17	9,13,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	3,7,10,12,14,16,18	9,13,15,18	2^{-12}

Table 0.280 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	3,7,10,17,18	9,11,17,18	2^{-1}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	3,7,10,16	9,11	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,7,10,17	9,11,15,17	2^{-1}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	3,7,10,16,18	9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	3,7,10,14	9,11	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	3,7,10,14,16,17,18	9,11,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	3,7,10,14,18	9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	3,7,10,14,16,17	9,11,15,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	3,7,10,17	9,11,13,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	3,7,10,16,18	9,11,13,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,7,10,17,18	9,11,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,7,10,16	9,11,13,15	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	3,7,10,14,18	9,11,13,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	3,7,10,14,16,17	9,11,13,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	3,7,10,14	9,11,13,15	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	3,7,10,14,16,17,18	9,11,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	3,7,10,12	9,11	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	3,7,10,12,16,17,18	9,11,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	3,7,10,12,18	9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	3,7,10,12,16,17	9,11,15,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	3,7,10,12,14,17,18	9,11,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	3,7,10,12,14,16	9,11	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	3,7,10,12,14,17	9,11,15,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	3,7,10,12,14,16,18	9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	3,7,10,12,18	9,11,13,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	3,7,10,12,16,17	9,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	3,7,10,12	9,11,13,15	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	3,7,10,12,16,17,18	9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	3,7,10,12,14,17	9,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	3,7,10,12,14,16,18	9,11,13,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	3,7,10,12,14,17,18	9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	3,7,10,12,14,16	9,11,13,15	2^{-23}

Table 0.281 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	3,7,17,18	8,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	3,7,16	8	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	3,7,17	8,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	3,7,16,18	8,15,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	3,7,14	8	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	3,7,14,16,17,18	8,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	3,7,14,18	8,15,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	3,7,14,16,17	8,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	3,7,17	8,13,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	3,7,16,18	8,13,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	3,7,17,18	8,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	3,7,16	8,13,15	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	3,7,14,18	8,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	3,7,14,16,17	8,13,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	3,7,14	8,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	3,7,14,16,17,18	8,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	3,7,12	8	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	3,7,12,16,17,18	8,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	3,7,12,18	8,15,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	3,7,12,16,17	8,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	3,7,12,14,17,18	8,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	3,7,12,14,16	8	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	3,7,12,14,17	8,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	3,7,12,14,16,18	8,15,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	3,7,12,18	8,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	3,7,12,16,17	8,13,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	3,7,12	8,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	3,7,12,16,17,18	8,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	3,7,12,14,17	8,13,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	3,7,12,14,16,18	8,13,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	3,7,12,14,17,18	8,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	3,7,12,14,16	8,13,15	$2^{-6.5}$

Table 0.282 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	3,7,17	8,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	3,7,16,18	8,11,18	2^{-1}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	3,7,17,18	8,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,7,16	8,11,15	2^{-1}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	3,7,14,18	8,11,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	3,7,14,16,17	8,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	3,7,14	8,11,15	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	3,7,14,16,17,18	8,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	3,7,17,18	8,11,13,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	3,7,16	8,11,13	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,7,17	8,11,13,15,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,7,16,18	8,11,13,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	3,7,14	8,11,13	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	3,7,14,16,17,18	8,11,13,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	3,7,14,18	8,11,13,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	3,7,14,16,17	8,11,13,15,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	3,7,12,18	8,11,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	3,7,12,16,17	8,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	3,7,12	8,11,15	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	3,7,12,16,17,18	8,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	3,7,12,14,17	8,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	3,7,12,14,16,18	8,11,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	3,7,12,14,17,18	8,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	3,7,12,14,16	8,11,15	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	3,7,12	8,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	3,7,12,16,17,18	8,11,13,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	3,7,12,18	8,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	3,7,12,16,17	8,11,13,15,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	3,7,12,14,17,18	8,11,13,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	3,7,12,14,16	8,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	3,7,12,14,17	8,11,13,15,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	3,7,12,14,16,18	8,11,13,15,18	$2^{-17.5}$

Table 0.283 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	3,7,10	8	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	3,7,10,16,17,18	8,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	3,7,10,18	8,15,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	3,7,10,16,17	8,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	3,7,10,14,17,18	8,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	3,7,10,14,16	8	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	3,7,10,14,17	8,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	3,7,10,14,16,18	8,15,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	3,7,10,18	8,13,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	3,7,10,16,17	8,13,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	3,7,10	8,13,15	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	3,7,10,16,17,18	8,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	3,7,10,14,17	8,13,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	3,7,10,14,16,18	8,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	3,7,10,14,17,18	8,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	3,7,10,14,16	8,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	3,7,10,12,17,18	8,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	3,7,10,12,16	8	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	3,7,10,12,17	8,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	3,7,10,12,16,18	8,15,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	3,7,10,12,14	8	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	3,7,10,12,14,16,17,18	8,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	3,7,10,12,14,18	8,15,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	3,7,10,12,14,16,17	8,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	3,7,10,12,17	8,13,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	3,7,10,12,16,18	8,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	3,7,10,12,17,18	8,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	3,7,10,12,16	8,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	3,7,10,12,14,18	8,13,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	3,7,10,12,14,16,17	8,13,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	3,7,10,12,14	8,13,15	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	3,7,10,12,14,16,17,18	8,13,15,17,18	2^{-23}

Table 0.284 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	3,7,10,18	8,11,18	2^{-34}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	3,7,10,16,17	8,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	3,7,10	8,11,15	2^{-34}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	3,7,10,16,17,18	8,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	3,7,10,14,17	8,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	3,7,10,14,16,18	8,11,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	3,7,10,14,17,18	8,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	3,7,10,14,16	8,11,15	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	3,7,10	8,11,13	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	3,7,10,16,17,18	8,11,13,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	3,7,10,18	8,11,13,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	3,7,10,16,17	8,11,13,15,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	3,7,10,14,17,18	8,11,13,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	3,7,10,14,16	8,11,13	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	3,7,10,14,17	8,11,13,15,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	3,7,10,14,16,18	8,11,13,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	3,7,10,12,17	8,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	3,7,10,12,16,18	8,11,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,7,10,12,17,18	8,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	3,7,10,12,16	8,11,15	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	3,7,10,12,14,18	8,11,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	3,7,10,12,14,16,17	8,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	3,7,10,12,14	8,11,15	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	3,7,10,12,14,16,17,18	8,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	3,7,10,12,17,18	8,11,13,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	3,7,10,12,16	8,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	3,7,10,12,17	8,11,13,15,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	3,7,10,12,16,18	8,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	3,7,10,12,14	8,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	3,7,10,12,14,16,17,18	8,11,13,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	3,7,10,12,14,18	8,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	3,7,10,12,14,16,17	8,11,13,15,17	2^{-12}

Table 0.285 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	3,7,17	8,9,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	3,7,16,18	8,9,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	3,7,17,18	8,9,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	3,7,16	8,9,15	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	3,7,14,18	8,9,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	3,7,14,16,17	8,9,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	3,7,14	8,9,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	3,7,14,16,17,18	8,9,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	3,7,17,18	8,9,13,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	3,7,16	8,9,13	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	3,7,17	8,9,13,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,7,16,18	8,9,13,15,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	3,7,14	8,9,13	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	3,7,14,16,17,18	8,9,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	3,7,14,18	8,9,13,15,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	3,7,14,16,17	8,9,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	3,7,12,18	8,9,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	3,7,12,16,17	8,9,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	3,7,12	8,9,15	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	3,7,12,16,17,18	8,9,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	3,7,12,14,17	8,9,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	3,7,12,14,16,18	8,9,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	3,7,12,14,17,18	8,9,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	3,7,12,14,16	8,9,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	3,7,12	8,9,13	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	3,7,12,16,17,18	8,9,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	3,7,12,18	8,9,13,15,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	3,7,12,16,17	8,9,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	3,7,12,14,17,18	8,9,13,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	3,7,12,14,16	8,9,13	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	3,7,12,14,17	8,9,13,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	3,7,12,14,16,18	8,9,13,15,18	2^{-23}

Table 0.286 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	3,7,17,18	8,9,11,17,18	2^{-34}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	3,7,16	8,9,11	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,7,17	8,9,11,15,17	2^{-34}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	3,7,16,18	8,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	3,7,14	8,9,11	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	3,7,14,16,17,18	8,9,11,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	3,7,14,18	8,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	3,7,14,16,17	8,9,11,15,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	3,7,17	8,9,11,13,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	3,7,16,18	8,9,11,13,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	3,7,17,18	8,9,11,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	3,7,16	8,9,11,13,15	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	3,7,14,18	8,9,11,13,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	3,7,14,16,17	8,9,11,13,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	3,7,14	8,9,11,13,15	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	3,7,14,16,17,18	8,9,11,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	3,7,12	8,9,11	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	3,7,12,16,17,18	8,9,11,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	3,7,12,18	8,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	3,7,12,16,17	8,9,11,15,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	3,7,12,14,17,18	8,9,11,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	3,7,12,14,16	8,9,11	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	3,7,12,14,17	8,9,11,15,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	3,7,12,14,16,18	8,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	3,7,12,18	8,9,11,13,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	3,7,12,16,17	8,9,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	3,7,12	8,9,11,13,15	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	3,7,12,16,17,18	8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	3,7,12,14,17	8,9,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	3,7,12,14,16,18	8,9,11,13,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	3,7,12,14,17,18	8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	3,7,12,14,16	8,9,11,13,15	2^{-12}

Table 0.287 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	3,7,10,18	8,9,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	3,7,10,16,17	8,9,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	3,7,10	8,9,15	$2^{-28.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	3,7,10,16,17,18	8,9,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	3,7,10,14,17	8,9,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	3,7,10,14,16,18	8,9,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	3,7,10,14,17,18	8,9,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	3,7,10,14,16	8,9,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	3,7,10	8,9,13	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	3,7,10,16,17,18	8,9,13,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,7,10,18	8,9,13,15,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	3,7,10,16,17	8,9,13,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	3,7,10,14,17,18	8,9,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	3,7,10,14,16	8,9,13	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	3,7,10,14,17	8,9,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	3,7,10,14,16,18	8,9,13,15,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	3,7,10,12,17	8,9,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	3,7,10,12,16,18	8,9,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	3,7,10,12,17,18	8,9,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	3,7,10,12,16	8,9,15	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	3,7,10,12,14,18	8,9,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	3,7,10,12,14,16,17	8,9,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	3,7,10,12,14	8,9,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	3,7,10,12,14,16,17,18	8,9,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	3,7,10,12,17,18	8,9,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	3,7,10,12,16	8,9,13	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	3,7,10,12,17	8,9,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	3,7,10,12,16,18	8,9,13,15,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	3,7,10,12,14	8,9,13	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	3,7,10,12,14,16,17,18	8,9,13,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	3,7,10,12,14,18	8,9,13,15,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	3,7,10,12,14,16,17	8,9,13,15,17	$2^{-6.5}$

Table 0.288 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	3,7,10	8,9,11	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	3,7,10,16,17,18	8,9,11,17,18	2^{-1}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	3,7,10,18	8,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	3,7,10,16,17	8,9,11,15,17	2^{-1}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	3,7,10,14,17,18	8,9,11,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	3,7,10,14,16	8,9,11	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	3,7,10,14,17	8,9,11,15,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	3,7,10,14,16,18	8,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	3,7,10,18	8,9,11,13,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	3,7,10,16,17	8,9,11,13,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	3,7,10	8,9,11,13,15	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	3,7,10,16,17,18	8,9,11,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	3,7,10,14,17	8,9,11,13,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	3,7,10,14,16,18	8,9,11,13,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	3,7,10,14,17,18	8,9,11,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	3,7,10,14,16	8,9,11,13,15	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	3,7,10,12,17,18	8,9,11,17,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	3,7,10,12,16	8,9,11	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	3,7,10,12,17	8,9,11,15,17	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	3,7,10,12,16,18	8,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	3,7,10,12,14	8,9,11	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	3,7,10,12,14,16,17,18	8,9,11,17,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	3,7,10,12,14,18	8,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	3,7,10,12,14,16,17	8,9,11,15,17	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	3,7,10,12,17	8,9,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	3,7,10,12,16,18	8,9,11,13,18	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	3,7,10,12,17,18	8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	3,7,10,12,16	8,9,11,13,15	2^{-12}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	3,7,10,12,14,18	8,9,11,13,18	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	3,7,10,12,14,16,17	8,9,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	3,7,10,12,14	8,9,11,13,15	2^{-23}
$(0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	3,7,10,12,14,16,17,18	8,9,11,13,15,17,18	$2^{-17.5}$

Table 0.289 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	3,17	6,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	3,16,18	6,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	3,17,18	6,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	3,16	6,15	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	3,14,18	6,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	3,14,16,17	6,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	3,14	6,15	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	3,14,16,17,18	6,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	3,17,18	6,13,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	3,16	6,13	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	3,17	6,13,15,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	3,16,18	6,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	3,14	6,13	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	3,14,16,17,18	6,13,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	3,14,18	6,13,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	3,14,16,17	6,13,15,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	3,12,18	6,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	3,12,16,17	6,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	3,12	6,15	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	3,12,16,17,18	6,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,12,14,17	6,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	3,12,14,16,18	6,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	3,12,14,17,18	6,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	3,12,14,16	6,15	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	3,12	6,13	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	3,12,16,17,18	6,13,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	3,12,18	6,13,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	3,12,16,17	6,13,15,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	3,12,14,17,18	6,13,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,12,14,16	6,13	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	3,12,14,17	6,13,15,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	3,12,14,16,18	6,13,15,18	$2^{-17.5}$

Table 0.290 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	3,17,18	6,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	3,16	6,11	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	3,17	6,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	3,16,18	6,11,15,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	3,14	6,11	2^{-1}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	3,14,16,17,18	6,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	3,14,18	6,11,15,18	2^{-1}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	3,14,16,17	6,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	3,17	6,11,13,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	3,16,18	6,11,13,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	3,17,18	6,11,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	3,16	6,11,13,15	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	3,14,18	6,11,13,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	3,14,16,17	6,11,13,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	3,14	6,11,13,15	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	3,14,16,17,18	6,11,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	3,12	6,11	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	3,12,16,17,18	6,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	3,12,18	6,11,15,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	3,12,16,17	6,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	3,12,14,17,18	6,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	3,12,14,16	6,11	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	3,12,14,17	6,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	3,12,14,16,18	6,11,15,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	3,12,18	6,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	3,12,16,17	6,11,13,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	3,12	6,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	3,12,16,17,18	6,11,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	3,12,14,17	6,11,13,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	3,12,14,16,18	6,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	3,12,14,17,18	6,11,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	3,12,14,16	6,11,13,15	$2^{-17.5}$

Table 0.291 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	3,10,18	6,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	3,10,16,17	6,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	3,10	6,15	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	3,10,16,17,18	6,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	3,10,14,17	6,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,10,14,16,18	6,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	3,10,14,17,18	6,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	3,10,14,16	6,15	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	3,10	6,13	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	3,10,16,17,18	6,13,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	3,10,18	6,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	3,10,16,17	6,13,15,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	3,10,14,17,18	6,13,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	3,10,14,16	6,13	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	3,10,14,17	6,13,15,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	3,10,14,16,18	6,13,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	3,10,12,17	6,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	3,10,12,16,18	6,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	3,10,12,17,18	6,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	3,10,12,16	6,15	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	3,10,12,14,18	6,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	3,10,12,14,16,17	6,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	3,10,12,14	6,15	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	3,10,12,14,16,17,18	6,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	3,10,12,17,18	6,13,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	3,10,12,16	6,13	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	3,10,12,17	6,13,15,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	3,10,12,16,18	6,13,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	3,10,12,14	6,13	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	3,10,12,14,16,17,18	6,13,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	3,10,12,14,18	6,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	3,10,12,14,16,17	6,13,15,17	2^{-23}

Table 0.292 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	3,10	6,11	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	3,10,16,17,18	6,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	3,10,18	6,11,15,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	3,10,16,17	6,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	3,10,14,17,18	6,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	3,10,14,16	6,11	2^{-34}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	3,10,14,17	6,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	3,10,14,16,18	6,11,15,18	2^{-34}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	3,10,18	6,11,13,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	3,10,16,17	6,11,13,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	3,10	6,11,13,15	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	3,10,16,17,18	6,11,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	3,10,14,17	6,11,13,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	3,10,14,16,18	6,11,13,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	3,10,14,17,18	6,11,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	3,10,14,16	6,11,13,15	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	3,10,12,17,18	6,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	3,10,12,16	6,11	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	3,10,12,17	6,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	3,10,12,16,18	6,11,15,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	3,10,12,14	6,11	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	3,10,12,14,16,17,18	6,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	3,10,12,14,18	6,11,15,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	3,10,12,14,16,17	6,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	3,10,12,17	6,11,13,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	3,10,12,16,18	6,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	3,10,12,17,18	6,11,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	3,10,12,16	6,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	3,10,12,14,18	6,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	3,10,12,14,16,17	6,11,13,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	3,10,12,14	6,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	3,10,12,14,16,17,18	6,11,13,15,17,18	2^{-23}

Table 0.293 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	3,17,18	6,9,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	3,16	6,9	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	3,17	6,9,15,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	3,16,18	6,9,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	3,14	6,9	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	3,14,16,17,18	6,9,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	3,14,18	6,9,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	3,14,16,17	6,9,15,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	3,17	6,9,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	3,16,18	6,9,13,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	3,17,18	6,9,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	3,16	6,9,13,15	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	3,14,18	6,9,13,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	3,14,16,17	6,9,13,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	3,14	6,9,13,15	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	3,14,16,17,18	6,9,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	3,12	6,9	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	3,12,16,17,18	6,9,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	3,12,18	6,9,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	3,12,16,17	6,9,15,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	3,12,14,17,18	6,9,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	3,12,14,16	6,9	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	3,12,14,17	6,9,15,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	3,12,14,16,18	6,9,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	3,12,18	6,9,13,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	3,12,16,17	6,9,13,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	3,12	6,9,13,15	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	3,12,16,17,18	6,9,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	3,12,14,17	6,9,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	3,12,14,16,18	6,9,13,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	3,12,14,17,18	6,9,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	3,12,14,16	6,9,13,15	2^{-23}

Table 0.294 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	3,17	6,9,11,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	3,16,18	6,9,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	3,17,18	6,9,11,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	3,16	6,9,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	3,14,18	6,9,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,14,16,17	6,9,11,17	2^{-34}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	3,14	6,9,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	3,14,16,17,18	6,9,11,15,17,18	2^{-34}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	3,17,18	6,9,11,13,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	3,16	6,9,11,13	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	3,17	6,9,11,13,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	3,16,18	6,9,11,13,15,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	3,14	6,9,11,13	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	3,14,16,17,18	6,9,11,13,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	3,14,18	6,9,11,13,15,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	3,14,16,17	6,9,11,13,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	3,12,18	6,9,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	3,12,16,17	6,9,11,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	3,12	6,9,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	3,12,16,17,18	6,9,11,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	3,12,14,17	6,9,11,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	3,12,14,16,18	6,9,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	3,12,14,17,18	6,9,11,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	3,12,14,16	6,9,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	3,12	6,9,11,13	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	3,12,16,17,18	6,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	3,12,18	6,9,11,13,15,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	3,12,16,17	6,9,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,12,14,17,18	6,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	3,12,14,16	6,9,11,13	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	3,12,14,17	6,9,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	3,12,14,16,18	6,9,11,13,15,18	2^{-23}

Table 0.295 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	3,10	6,9	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	3,10,16,17,18	6,9,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	3,10,18	6,9,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	3,10,16,17	6,9,15,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	3,10,14,17,18	6,9,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	3,10,14,16	6,9	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	3,10,14,17	6,9,15,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	3,10,14,16,18	6,9,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	3,10,18	6,9,13,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	3,10,16,17	6,9,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	3,10	6,9,13,15	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	3,10,16,17,18	6,9,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	3,10,14,17	6,9,13,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	3,10,14,16,18	6,9,13,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	3,10,14,17,18	6,9,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	3,10,14,16	6,9,13,15	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	3,10,12,17,18	6,9,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	3,10,12,16	6,9	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	3,10,12,17	6,9,15,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	3,10,12,16,18	6,9,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	3,10,12,14	6,9	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	3,10,12,14,16,17,18	6,9,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	3,10,12,14,18	6,9,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	3,10,12,14,16,17	6,9,15,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	3,10,12,17	6,9,13,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	3,10,12,16,18	6,9,13,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	3,10,12,17,18	6,9,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	3,10,12,16	6,9,13,15	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	3,10,12,14,18	6,9,13,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	3,10,12,14,16,17	6,9,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	3,10,12,14	6,9,13,15	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	3,10,12,14,16,17,18	6,9,13,15,17,18	$2^{-17.5}$

Table 0.296 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	3,10,18	6,9,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	3,10,16,17	6,9,11,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	3,10	6,9,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	3,10,16,17,18	6,9,11,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	3,10,14,17	6,9,11,17	2^{-1}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	3,10,14,16,18	6,9,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	3,10,14,17,18	6,9,11,15,17,18	2^{-1}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	3,10,14,16	6,9,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	3,10	6,9,11,13	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	3,10,16,17,18	6,9,11,13,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	3,10,18	6,9,11,13,15,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	3,10,16,17	6,9,11,13,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	3,10,14,17,18	6,9,11,13,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	3,10,14,16	6,9,11,13	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	3,10,14,17	6,9,11,13,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	3,10,14,16,18	6,9,11,13,15,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	3,10,12,17	6,9,11,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	3,10,12,16,18	6,9,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	3,10,12,17,18	6,9,11,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	3,10,12,16	6,9,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	3,10,12,14,18	6,9,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	3,10,12,17,18	6,9,11,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	3,10,12,14,16,17	6,9,11,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	3,10,12,14	6,9,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	3,10,12,14,16,17,18	6,9,11,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	3,10,12,17,18	6,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	3,10,12,16	6,9,11,13	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	3,10,12,17	6,9,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	3,10,12,16,18	6,9,11,13,15,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	3,10,12,14	6,9,11,13	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,10,12,14,16,17,18	6,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	3,10,12,14,18	6,9,11,13,15,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	3,10,12,14,16,17	6,9,11,13,15,17	$2^{-17.5}$

Table 0.297 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	3,18	6,8,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	3,16,17	6,8,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	3	6,8,15	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	3,16,17,18	6,8,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	3,14,17	6,8,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	3,14,16,18	6,8,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	3,14,17,18	6,8,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	3,14,16	6,8,15	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	3	6,8,13	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	3,16,17,18	6,8,13,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	3,18	6,8,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	3,16,17	6,8,13,15,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	3,14,17,18	6,8,13,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	3,14,16	6,8,13	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	3,14,17	6,8,13,15,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	3,14,16,18	6,8,13,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	3,12,17	6,8,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	3,12,16,18	6,8,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	3,12,17,18	6,8,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	3,12,16	6,8,15	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	3,12,14,18	6,8,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	3,12,14,16,17	6,8,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	3,12,14	6,8,15	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	3,12,14,16,17,18	6,8,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	3,12,17,18	6,8,13,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	3,12,16	6,8,13	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	3,12,17	6,8,13,15,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	3,12,16,18	6,8,13,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	3,12,14	6,8,13	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	3,12,14,16,17,18	6,8,13,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	3,12,14,18	6,8,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	3,12,14,16,17	6,8,13,15,17	2^{-12}

Table 0.298 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	3	6,8,11	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	3,16,17,18	6,8,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	3,18	6,8,11,15,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	3,16,17	6,8,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	3,14,17,18	6,8,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	3,14,16	6,8,11	2^{-1}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	3,14,17	6,8,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	3,14,16,18	6,8,11,15,18	2^{-1}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	3,18	6,8,11,13,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	3,16,17	6,8,11,13,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	3	6,8,11,13,15	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	3,16,17,18	6,8,11,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	3,14,17	6,8,11,13,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	3,14,16,18	6,8,11,13,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	3,14,17,18	6,8,11,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	3,14,16	6,8,11,13,15	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	3,12,17,18	6,8,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	3,12,16	6,8,11	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	3,12,17	6,8,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	3,12,16,18	6,8,11,15,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	3,12,14	6,8,11	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	3,12,14,16,17,18	6,8,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	3,12,14,18	6,8,11,15,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	3,12,14,16,17	6,8,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	3,12,17	6,8,11,13,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	3,12,16,18	6,8,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	3,12,17,18	6,8,11,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	3,12,16	6,8,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,12,14,18	6,8,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	3,12,14,16,17	6,8,11,13,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	3,12,14	6,8,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	3,12,14,16,17,18	6,8,11,13,15,17,18	2^{-12}

Table 0.299 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(2)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	3,10,17	6,8,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	3,10,16,18	6,8,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	3,10,17,18	6,8,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	3,10,16	6,8,15	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	3,10,14,18	6,8,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	3,10,14,16,17	6,8,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	3,10,14	6,8,15	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	3,10,14,16,17,18	6,8,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	3,10,17,18	6,8,13,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	3,10,16	6,8,13	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	3,10,17	6,8,13,15,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	3,10,16,18	6,8,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	3,10,14	6,8,13	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	3,10,14,16,17,18	6,8,13,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	3,10,14,18	6,8,13,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	3,10,14,16,17	6,8,13,15,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	3,10,12,18	6,8,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	3,10,12,16,17	6,8,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	3,10,12	6,8,15	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	3,10,12,16,17,18	6,8,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	3,10,12,14,17	6,8,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	3,10,12,14,16,18	6,8,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	3,10,12,14,17,18	6,8,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	3,10,12,14,16	6,8,15	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	3,10,12	6,8,13	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	3,10,12,16,17,18	6,8,13,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	3,10,12,18	6,8,13,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	3,10,12,16,17	6,8,13,15,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	3,10,12,14,17,18	6,8,13,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	3,10,12,14,16	6,8,13	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	3,10,12,14,17	6,8,13,15,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	3,10,12,14,16,18	6,8,13,15,18	$2^{-17.5}$

Table 0.300 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	3,10,17,18	6,8,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	3,10,16	6,8,11	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	3,10,17	6,8,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	3,10,16,18	6,8,11,15,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	3,10,14	6,8,11	2^{-34}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	3,10,14,16,17,18	6,8,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	3,10,14,18	6,8,11,15,18	2^{-34}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	3,10,14,16,17	6,8,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	3,10,17	6,8,11,13,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	3,10,16,18	6,8,11,13,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	3,10,17,18	6,8,11,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	3,10,16	6,8,11,13,15	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	3,10,14,18	6,8,11,13,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	3,10,14,16,17	6,8,11,13,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	3,10,14	6,8,11,13,15	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	3,10,14,16,17,18	6,8,11,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	3,10,12	6,8,11	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	3,10,12,16,17,18	6,8,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	3,10,12,18	6,8,11,15,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	3,10,12,16,17	6,8,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	3,10,12,14,17,18	6,8,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	3,10,12,14,16	6,8,11	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	3,10,12,14,17	6,8,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	3,10,12,14,16,18	6,8,11,15,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	3,10,12,18	6,8,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	3,10,12,16,17	6,8,11,13,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	3,10,12	6,8,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	3,10,12,16,17,18	6,8,11,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	3,10,12,14,17	6,8,11,13,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,10,12,14,16,18	6,8,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	3,10,12,14,17,18	6,8,11,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	3,10,12,14,16	6,8,11,13,15	$2^{-17.5}$

Table 0.301 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	3	6,8,9	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	3,16,17,18	6,8,9,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	3,18	6,8,9,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	3,16,17	6,8,9,15,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,14,17,18	6,8,9,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	3,14,16	6,8,9	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	3,14,17	6,8,9,15,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	3,14,16,18	6,8,9,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	3,18	6,8,9,13,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	3,16,17	6,8,9,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	3	6,8,9,13,15	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	3,16,17,18	6,8,9,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	3,14,17	6,8,9,13,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	3,14,16,18	6,8,9,13,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	3,14,17,18	6,8,9,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	3,14,16	6,8,9,13,15	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	3,12,17,18	6,8,9,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	3,12,16	6,8,9	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	3,12,17	6,8,9,15,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	3,12,16,18	6,8,9,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	3,12,14	6,8,9	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	3,12,14,16,17,18	6,8,9,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	3,12,14,18	6,8,9,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	3,12,14,16,17	6,8,9,15,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	3,12,17	6,8,9,13,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	3,12,16,18	6,8,9,13,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	3,12,17,18	6,8,9,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	3,12,16	6,8,9,13,15	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	3,12,14,18	6,8,9,13,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	3,12,14,16,17	6,8,9,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	3,12,14	6,8,9,13,15	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	3,12,14,16,17,18	6,8,9,13,15,17,18	$2^{-17.5}$

Table 0.302 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	3,18	6,8,9,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	3,16,17	6,8,9,11,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	3	6,8,9,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	3,16,17,18	6,8,9,11,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	3,14,17	6,8,9,11,17	2^{-34}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	3,14,16,18	6,8,9,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	3,14,17,18	6,8,9,11,15,17,18	2^{-34}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	3,14,16	6,8,9,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	3	6,8,9,11,13	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	3,16,17,18	6,8,9,11,13,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	3,18	6,8,9,11,13,15,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	3,16,17	6,8,9,11,13,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	3,14,17,18	6,8,9,11,13,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	3,14,16	6,8,9,11,13	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	3,14,17	6,8,9,11,13,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	3,14,16,18	6,8,9,11,13,15,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	3,12,17	6,8,9,11,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	3,12,16,18	6,8,9,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	3,12,17,18	6,8,9,11,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	3,12,16	6,8,9,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	3,12,14,18	6,8,9,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	3,12,14,16,17	6,8,9,11,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	3,12,14	6,8,9,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	3,12,14,16,17,18	6,8,9,11,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	3,12,17,18	6,8,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	3,12,16	6,8,9,11,13	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	3,12,17	6,8,9,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	3,12,16,18	6,8,9,11,13,15,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	3,12,14	6,8,9,11,13	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	3,12,14,16,17,18	6,8,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	3,12,14,18	6,8,9,11,13,15,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	3,12,14,16,17	6,8,9,11,13,15,17	$2^{-17.5}$

Table 0.303 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	3,10,17,18	6,8,9,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	3,10,16	6,8,9	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	3,10,17	6,8,9,15,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	3,10,16,18	6,8,9,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	3,10,14	6,8,9	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	3,10,14,16,17,18	6,8,9,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	3,10,14,18	6,8,9,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	3,10,14,16,17	6,8,9,15,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	3,10,17	6,8,9,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	3,10,16,18	6,8,9,13,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	3,10,17,18	6,8,9,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	3,10,16	6,8,9,13,15	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	3,10,14,18	6,8,9,13,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	3,10,14,16,17	6,8,9,13,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	3,10,14	6,8,9,13,15	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	3,10,14,16,17,18	6,8,9,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	3,10,12	6,8,9	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	3,10,12,16,17,18	6,8,9,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	3,10,12,18	6,8,9,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	3,10,12,16,17	6,8,9,15,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	3,10,12,14,17,18	6,8,9,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,10,12,14,16	6,8,9	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	3,10,12,14,17	6,8,9,15,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	3,10,12,14,16,18	6,8,9,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	3,10,12,18	6,8,9,13,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	3,10,12,16,17	6,8,9,13,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	3,10,12	6,8,9,13,15	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	3,10,12,16,17,18	6,8,9,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,10,12,14,17	6,8,9,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,10,12,14,16,18	6,8,9,13,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	3,10,12,14,17,18	6,8,9,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	3,10,12,14,16	6,8,9,13,15	2^{-12}

Table 0.304 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	3,10,17	6,8,9,11,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	3,10,16,18	6,8,9,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	3,10,17,18	6,8,9,11,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	3,10,16	6,8,9,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	3,10,14,18	6,8,9,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	3,10,14,16,17	6,8,9,11,17	2^{-1}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	3,10,14	6,8,9,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	3,10,14,16,17,18	6,8,9,11,15,17,18	2^{-1}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	3,10,17,18	6,8,9,11,13,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	3,10,16	6,8,9,11,13	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	3,10,17	6,8,9,11,13,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	3,10,16,18	6,8,9,11,13,15,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	3,10,14	6,8,9,11,13	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	3,10,14,16,17,18	6,8,9,11,13,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	3,10,14,18	6,8,9,11,13,15,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	3,10,14,16,17	6,8,9,11,13,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	3,10,12,18	6,8,9,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	3,10,12,16,17	6,8,9,11,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	3,10,12	6,8,9,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	3,10,12,16,17,18	6,8,9,11,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	3,10,12,14,17	6,8,9,11,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	3,10,12,14,16,18	6,8,9,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	3,10,12,14,17,18	6,8,9,11,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	3,10,12,14,16	6,8,9,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	3,10,12	6,8,9,11,13	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	3,10,12,16,17,18	6,8,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	3,10,12,18	6,8,9,11,13,15,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	3,10,12,16,17	6,8,9,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	3,10,12,14,17,18	6,8,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	3,10,12,14,16	6,8,9,11,13	2^{-12}
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	3,10,12,14,17	6,8,9,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	3,10,12,14,16,18	6,8,9,11,13,15,18	2^{-12}

Table 0.305 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	3,7,17,18	6,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	3,7,16	6	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	3,7,17	6,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	3,7,16,18	6,15,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	3,7,14	6	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	3,7,14,16,17,18	6,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	3,7,14,18	6,15,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	3,7,14,16,17	6,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	3,7,17	6,13,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	3,7,16,18	6,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	3,7,17,18	6,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	3,7,16	6,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	3,7,14,18	6,13,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	3,7,14,16,17	6,13,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	3,7,14	6,13,15	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	3,7,14,16,17,18	6,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	3,7,12	6	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	3,7,12,16,17,18	6,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	3,7,12,18	6,15,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	3,7,12,16,17	6,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	3,7,12,14,17,18	6,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	3,7,12,14,16	6	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	3,7,12,14,17	6,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	3,7,12,14,16,18	6,15,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	3,7,12,18	6,13,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	3,7,12,16,17	6,13,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	3,7,12	6,13,15	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	3,7,12,16,17,18	6,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	3,7,12,14,17	6,13,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	3,7,12,14,16,18	6,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,7,12,14,17,18	6,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	3,7,12,14,16	6,13,15	$2^{-17.5}$

Table 0.306 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	3,7,17	6,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	3,7,16,18	6,11,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	3,7,17,18	6,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	3,7,16	6,11,15	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	3,7,14,18	6,11,18	2^{-1}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	3,7,14,16,17	6,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	3,7,14	6,11,15	2^{-1}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	3,7,14,16,17,18	6,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	3,7,17,18	6,11,13,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	3,7,16	6,11,13	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	3,7,17	6,11,13,15,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	3,7,16,18	6,11,13,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	3,7,14	6,11,13	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	3,7,14,16,17,18	6,11,13,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	3,7,14,18	6,11,13,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	3,7,14,16,17	6,11,13,15,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	3,7,12,18	6,11,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	3,7,12,16,17	6,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	3,7,12	6,11,15	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	3,7,12,16,17,18	6,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	3,7,12,14,17	6,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	3,7,12,14,16,18	6,11,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	3,7,12,14,17,18	6,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	3,7,12,14,16	6,11,15	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	3,7,12	6,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	3,7,12,16,17,18	6,11,13,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	3,7,12,18	6,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	3,7,12,16,17	6,11,13,15,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	3,7,12,14,17,18	6,11,13,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	3,7,12,14,16	6,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	3,7,12,14,17	6,11,13,15,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	3,7,12,14,16,18	6,11,13,15,18	$2^{-17.5}$

Table 0.307 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	3,7,10	6	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	3,7,10,16,17,18	6,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	3,7,10,18	6,15,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	3,7,10,16,17	6,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	3,7,10,14,17,18	6,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	3,7,10,14,16	6	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	3,7,10,14,17	6,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	3,7,10,14,16,18	6,15,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	3,7,10,18	6,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	3,7,10,16,17	6,13,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	3,7,10	6,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	3,7,10,16,17,18	6,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	3,7,10,14,17	6,13,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	3,7,10,14,16,18	6,13,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	3,7,10,14,17,18	6,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	3,7,10,14,16	6,13,15	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	3,7,10,12,17,18	6,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	3,7,10,12,16	6	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	3,7,10,12,17	6,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	3,7,10,12,16,18	6,15,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	3,7,10,12,14	6	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	3,7,10,12,14,16,17,18	6,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	3,7,10,12,14,18	6,15,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	3,7,10,12,14,16,17	6,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	3,7,10,12,17	6,13,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	3,7,10,12,16,18	6,13,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	3,7,10,12,17,18	6,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	3,7,10,12,16	6,13,15	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	3,7,10,12,14,18	6,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	3,7,10,12,14,16,17	6,13,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	3,7,10,12,14	6,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,7,10,12,14,16,17,18	6,13,15,17,18	2^{-23}

Table 0.308 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	3,7,10,18	6,11,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	3,7,10,16,17	6,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	3,7,10	6,11,15	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	3,7,10,16,17,18	6,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	3,7,10,14,17	6,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	3,7,10,14,16,18	6,11,18	2^{-34}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	3,7,10,14,17,18	6,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	3,7,10,14,16	6,11,15	2^{-34}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	3,7,10	6,11,13	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	3,7,10,16,17,18	6,11,13,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	3,7,10,18	6,11,13,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	3,7,10,16,17	6,11,13,15,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	3,7,10,14,17,18	6,11,13,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	3,7,10,14,16	6,11,13	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	3,7,10,14,17	6,11,13,15,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	3,7,10,14,16,18	6,11,13,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	3,7,10,12,17	6,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	3,7,10,12,16,18	6,11,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	3,7,10,12,17,18	6,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	3,7,10,12,16	6,11,15	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	3,7,10,12,14,18	6,11,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	3,7,10,12,14,16,17	6,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	3,7,10,12,14	6,11,15	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	3,7,10,12,14,16,17,18	6,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	3,7,10,12,17,18	6,11,13,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	3,7,10,12,16	6,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	3,7,10,12,17	6,11,13,15,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	3,7,10,12,16,18	6,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	3,7,10,12,14	6,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	3,7,10,12,14,16,17,18	6,11,13,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	3,7,10,12,14,18	6,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	3,7,10,12,14,16,17	6,11,13,15,17	2^{-23}

Table 0.309 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	3,7,17	6,9,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	3,7,16,18	6,9,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	3,7,17,18	6,9,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	3,7,16	6,9,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	3,7,14,18	6,9,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	3,7,14,16,17	6,9,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	3,7,14	6,9,15	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	3,7,14,16,17,18	6,9,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	3,7,17,18	6,9,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	3,7,16	6,9,13	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	3,7,17	6,9,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	3,7,16,18	6,9,13,15,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	3,7,14	6,9,13	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	3,7,14,16,17,18	6,9,13,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	3,7,14,18	6,9,13,15,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	3,7,14,16,17	6,9,13,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	3,7,12,18	6,9,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	3,7,12,16,17	6,9,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	3,7,12	6,9,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	3,7,12,16,17,18	6,9,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	3,7,12,14,17	6,9,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	3,7,12,14,16,18	6,9,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	3,7,12,14,17,18	6,9,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	3,7,12,14,16	6,9,15	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	3,7,12	6,9,13	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	3,7,12,16,17,18	6,9,13,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	3,7,12,18	6,9,13,15,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	3,7,12,16,17	6,9,13,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	3,7,12,14,17,18	6,9,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	3,7,12,14,16	6,9,13	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	3,7,12,14,17	6,9,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	3,7,12,14,16,18	6,9,13,15,18	2^{-23}

Table 0.310 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	3,7,17,18	6,9,11,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	3,7,16	6,9,11	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	3,7,17	6,9,11,15,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	3,7,16,18	6,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	3,7,14	6,9,11	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	3,7,14,16,17,18	6,9,11,17,18	2^{-34}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	3,7,14,18	6,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	3,7,14,16,17	6,9,11,15,17	2^{-34}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	3,7,17	6,9,11,13,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	3,7,16,18	6,9,11,13,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	3,7,17,18	6,9,11,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	3,7,16	6,9,11,13,15	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	3,7,14,18	6,9,11,13,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	3,7,14,16,17	6,9,11,13,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	3,7,14	6,9,11,13,15	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	3,7,14,16,17,18	6,9,11,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	3,7,12	6,9,11	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	3,7,12,16,17,18	6,9,11,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	3,7,12,18	6,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	3,7,12,16,17	6,9,11,15,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	3,7,12,14,17,18	6,9,11,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	3,7,12,14,16	6,9,11	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,7,12,14,17	6,9,11,15,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	3,7,12,14,16,18	6,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	3,7,12,18	6,9,11,13,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	3,7,12,16,17	6,9,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	3,7,12	6,9,11,13,15	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	3,7,12,16,17,18	6,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	3,7,12,14,17	6,9,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	3,7,12,14,16,18	6,9,11,13,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,7,12,14,17,18	6,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,7,12,14,16	6,9,11,13,15	2^{-23}

Table 0.311 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	3,7,10,18	6,9,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	3,7,10,16,17	6,9,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	3,7,10	6,9,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	3,7,10,16,17,18	6,9,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	3,7,10,14,17	6,9,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	3,7,10,14,16,18	6,9,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	3,7,10,14,17,18	6,9,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	3,7,10,14,16	6,9,15	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	3,7,10	6,9,13	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	3,7,10,16,17,18	6,9,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	3,7,10,18	6,9,13,15,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	3,7,10,16,17	6,9,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	3,7,10,14,17,18	6,9,13,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	3,7,10,14,16	6,9,13	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	3,7,10,14,17	6,9,13,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	3,7,10,14,16,18	6,9,13,15,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	3,7,10,12,17	6,9,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	3,7,10,12,16,18	6,9,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	3,7,10,12,17,18	6,9,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	3,7,10,12,16	6,9,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	3,7,10,12,14,18	6,9,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	3,7,10,12,14,16,17	6,9,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	3,7,10,12,14	6,9,15	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	3,7,10,12,14,16,17,18	6,9,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	3,7,10,12,17,18	6,9,13,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	3,7,10,12,16	6,9,13	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	3,7,10,12,17	6,9,13,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	3,7,10,12,16,18	6,9,13,15,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	3,7,10,12,14	6,9,13	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	3,7,10,12,14,16,17,18	6,9,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	3,7,10,12,14,18	6,9,13,15,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	3,7,10,12,14,16,17	6,9,13,15,17	$2^{-17.5}$

Table 0.312 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	3,7,10	6,9,11	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	3,7,10,16,17,18	6,9,11,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	3,7,10,18	6,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	3,7,10,16,17	6,9,11,15,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	3,7,10,14,17,18	6,9,11,17,18	2^{-1}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	3,7,10,14,16	6,9,11	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	3,7,10,14,17	6,9,11,15,17	2^{-1}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,7,10,14,16,18	6,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	3,7,10,18	6,9,11,13,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	3,7,10,16,17	6,9,11,13,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	3,7,10	6,9,11,13,15	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	3,7,10,16,17,18	6,9,11,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	3,7,10,14,17	6,9,11,13,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	3,7,10,14,16,18	6,9,11,13,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	3,7,10,14,17,18	6,9,11,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	3,7,10,14,16	6,9,11,13,15	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	3,7,10,12,17,18	6,9,11,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	3,7,10,12,16	6,9,11	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	3,7,10,12,17	6,9,11,15,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	3,7,10,12,16,18	6,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	3,7,10,12,14	6,9,11	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	3,7,10,12,14,16,17,18	6,9,11,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	3,7,10,12,14,18	6,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	3,7,10,12,14,16,17	6,9,11,15,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	3,7,10,12,17	6,9,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	3,7,10,12,16,18	6,9,11,13,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	3,7,10,12,17,18	6,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	3,7,10,12,16	6,9,11,13,15	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	3,7,10,12,14,18	6,9,11,13,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	3,7,10,12,14,16,17	6,9,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	3,7,10,12,14	6,9,11,13,15	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	3,7,10,12,14,16,17,18	6,9,11,13,15,17,18	$2^{-17.5}$

Table 0.313 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	3,7	6,8	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	3,7,16,17,18	6,8,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	3,7,18	6,8,15,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	3,7,16,17	6,8,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	3,7,14,17,18	6,8,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	3,7,14,16	6,8	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	3,7,14,17	6,8,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	3,7,14,16,18	6,8,15,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	3,7,18	6,8,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	3,7,16,17	6,8,13,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	3,7	6,8,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	3,7,16,17,18	6,8,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	3,7,14,17	6,8,13,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	3,7,14,16,18	6,8,13,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	3,7,14,17,18	6,8,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	3,7,14,16	6,8,13,15	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	3,7,12,17,18	6,8,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	3,7,12,16	6,8	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	3,7,12,17	6,8,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	3,7,12,16,18	6,8,15,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	3,7,12,14	6,8	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	3,7,12,14,16,17,18	6,8,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	3,7,12,14,18	6,8,15,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	3,7,12,14,16,17	6,8,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	3,7,12,17	6,8,13,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	3,7,12,16,18	6,8,13,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	3,7,12,17,18	6,8,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	3,7,12,16	6,8,13,15	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	3,7,12,14,18	6,8,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	3,7,12,14,16,17	6,8,13,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	3,7,12,14	6,8,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	3,7,12,14,16,17,18	6,8,13,15,17,18	2^{-12}

Table 0.314 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	3,7,18	6,8,11,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	3,7,16,17	6,8,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	3,7	6,8,11,15	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	3,7,16,17,18	6,8,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	3,7,14,17	6,8,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	3,7,14,16,18	6,8,11,18	2^{-1}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,7,14,17,18	6,8,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	3,7,14,16	6,8,11,15	2^{-1}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	3,7	6,8,11,13	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	3,7,16,17,18	6,8,11,13,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	3,7,18	6,8,11,13,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	3,7,16,17	6,8,11,13,15,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	3,7,14,17,18	6,8,11,13,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	3,7,14,16	6,8,11,13	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	3,7,14,17	6,8,11,13,15,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	3,7,14,16,18	6,8,11,13,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	3,7,12,17	6,8,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	3,7,12,16,18	6,8,11,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	3,7,12,17,18	6,8,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	3,7,12,16	6,8,11,15	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	3,7,12,14,18	6,8,11,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	3,7,12,14,16,17	6,8,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	3,7,12,14	6,8,11,15	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	3,7,12,14,16,17,18	6,8,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	3,7,12,17,18	6,8,11,13,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	3,7,12,16	6,8,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	3,7,12,17	6,8,11,13,15,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	3,7,12,16,18	6,8,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	3,7,12,14	6,8,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	3,7,12,14,16,17,18	6,8,11,13,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	3,7,12,14,18	6,8,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	3,7,12,14,16,17	6,8,11,13,15,17	2^{-12}

Table 0.315 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	3,7,10,17,18	6,8,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	3,7,10,16	6,8	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	3,7,10,17	6,8,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	3,7,10,16,18	6,8,15,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	3,7,10,14	6,8	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	3,7,10,14,16,17,18	6,8,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	3,7,10,14,18	6,8,15,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	3,7,10,14,16,17	6,8,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	3,7,10,17	6,8,13,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	3,7,10,16,18	6,8,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	3,7,10,17,18	6,8,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	3,7,10,16	6,8,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	3,7,10,14,18	6,8,13,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	3,7,10,14,16,17	6,8,13,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	3,7,10,14	6,8,13,15	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	3,7,10,14,16,17,18	6,8,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	3,7,10,12	6,8	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	3,7,10,12,16,17,18	6,8,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	3,7,10,12,18	6,8,15,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	3,7,10,12,16,17	6,8,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	3,7,10,12,14,17,18	6,8,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	3,7,10,12,14,16	6,8	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	3,7,10,12,14,17	6,8,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	3,7,10,12,14,16,18	6,8,15,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	3,7,10,12,18	6,8,13,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	3,7,10,12,16,17	6,8,13,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	3,7,10,12	6,8,13,15	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	3,7,10,12,16,17,18	6,8,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	3,7,10,12,14,17	6,8,13,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	3,7,10,12,14,16,18	6,8,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	3,7,10,12,14,17,18	6,8,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	3,7,10,12,14,16	6,8,13,15	$2^{-17.5}$

Table 0.316 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	3,7,10,17	6,8,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	3,7,10,16,18	6,8,11,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	3,7,10,17,18	6,8,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	3,7,10,16	6,8,11,15	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	3,7,10,14,18	6,8,11,18	2^{-34}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	3,7,10,14,16,17	6,8,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	3,7,10,14	6,8,11,15	2^{-34}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	3,7,10,14,16,17,18	6,8,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	3,7,10,17,18	6,8,11,13,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	3,7,10,16	6,8,11,13	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	3,7,10,17	6,8,11,13,15,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	3,7,10,16,18	6,8,11,13,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	3,7,10,14	6,8,11,13	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	3,7,10,14,16,17,18	6,8,11,13,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	3,7,10,14,18	6,8,11,13,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	3,7,10,14,16,17	6,8,11,13,15,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	3,7,10,12,18	6,8,11,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	3,7,10,12,16,17	6,8,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	3,7,10,12	6,8,11,15	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	3,7,10,12,16,17,18	6,8,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	3,7,10,12,14,17	6,8,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	3,7,10,12,14,16,18	6,8,11,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	3,7,10,12,14,17,18	6,8,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,7,10,12,14,16	6,8,11,15	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	3,7,10,12	6,8,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	3,7,10,12,16,17,18	6,8,11,13,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	3,7,10,12,18	6,8,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	3,7,10,12,16,17	6,8,11,13,15,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	3,7,10,12,14,17,18	6,8,11,13,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	3,7,10,12,14,16	6,8,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,7,10,12,14,17	6,8,11,13,15,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,7,10,12,14,16,18	6,8,11,13,15,18	$2^{-17.5}$

Table 0.317 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	3,7,18	6,8,9,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	3,7,16,17	6,8,9,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	3,7	6,8,9,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	3,7,16,17,18	6,8,9,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	3,7,14,17	6,8,9,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	3,7,14,16,18	6,8,9,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	3,7,14,17,18	6,8,9,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	3,7,14,16	6,8,9,15	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	3,7	6,8,9,13	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	3,7,16,17,18	6,8,9,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	3,7,18	6,8,9,13,15,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	3,7,16,17	6,8,9,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	3,7,14,17,18	6,8,9,13,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	3,7,14,16	6,8,9,13	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	3,7,14,17	6,8,9,13,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	3,7,14,16,18	6,8,9,13,15,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	3,7,12,17	6,8,9,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	3,7,12,16,18	6,8,9,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	3,7,12,17,18	6,8,9,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	3,7,12,16	6,8,9,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	3,7,12,14,18	6,8,9,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	3,7,12,14,16,17	6,8,9,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	3,7,12,14	6,8,9,15	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	3,7,12,14,16,17,18	6,8,9,15,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	3,7,12,17,18	6,8,9,13,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	3,7,12,16	6,8,9,13	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	3,7,12,17	6,8,9,13,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	3,7,12,16,18	6,8,9,13,15,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	3,7,12,14	6,8,9,13	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	3,7,12,14,16,17,18	6,8,9,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,7,12,14,18	6,8,9,13,15,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	3,7,12,14,16,17	6,8,9,13,15,17	$2^{-17.5}$

Table 0.318 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	3,7	6,8,9,11	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	3,7,16,17,18	6,8,9,11,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	3,7,18	6,8,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	3,7,16,17	6,8,9,11,15,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	3,7,14,17,18	6,8,9,11,17,18	2^{-34}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	3,7,14,16	6,8,9,11	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	3,7,14,17	6,8,9,11,15,17	2^{-34}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	3,7,14,16,18	6,8,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	3,7,18	6,8,9,11,13,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	3,7,16,17	6,8,9,11,13,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	3,7	6,8,9,11,13,15	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	3,7,16,17,18	6,8,9,11,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	3,7,14,17	6,8,9,11,13,17	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	3,7,14,16,18	6,8,9,11,13,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	3,7,14,17,18	6,8,9,11,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	3,7,14,16	6,8,9,11,13,15	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	3,7,12,17,18	6,8,9,11,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	3,7,12,16	6,8,9,11	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	3,7,12,17	6,8,9,11,15,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	3,7,12,16,18	6,8,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	3,7,12,14	6,8,9,11	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	3,7,12,14,16,17,18	6,8,9,11,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	3,7,12,14,18	6,8,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	3,7,12,14,16,17	6,8,9,11,15,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	3,7,12,17	6,8,9,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	3,7,12,16,18	6,8,9,11,13,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	3,7,12,17,18	6,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	3,7,12,16	6,8,9,11,13,15	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	3,7,12,14,18	6,8,9,11,13,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	3,7,12,14,16,17	6,8,9,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	3,7,12,14	6,8,9,11,13,15	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	3,7,12,14,16,17,18	6,8,9,11,13,15,17,18	$2^{-17.5}$

Table 0.319 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	3,7,10,17	6,8,9,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	3,7,10,16,18	6,8,9,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	3,7,10,17,18	6,8,9,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	3,7,10,16	6,8,9,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	3,7,10,14,18	6,8,9,18	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	3,7,10,14,16,17	6,8,9,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	3,7,10,14	6,8,9,15	$2^{-28.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	3,7,10,14,16,17,18	6,8,9,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	3,7,10,17,18	6,8,9,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	3,7,10,16	6,8,9,13	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	3,7,10,17	6,8,9,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	3,7,10,16,18	6,8,9,13,15,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	3,7,10,14	6,8,9,13	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	3,7,10,14,16,17,18	6,8,9,13,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	3,7,10,14,18	6,8,9,13,15,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	3,7,10,14,16,17	6,8,9,13,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	3,7,10,12,18	6,8,9,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	3,7,10,12,16,17	6,8,9,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	3,7,10,12	6,8,9,15	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	3,7,10,12,16,17,18	6,8,9,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	3,7,10,12,14,17	6,8,9,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	3,7,10,12,14,16,18	6,8,9,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	3,7,10,12,14,17,18	6,8,9,15,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	3,7,10,12,14,16	6,8,9,15	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	3,7,10,12	6,8,9,13	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	3,7,10,12,16,17,18	6,8,9,13,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	3,7,10,12,18	6,8,9,13,15,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	3,7,10,12,16,17	6,8,9,13,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	3,7,10,12,14,17,18	6,8,9,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	3,7,10,12,14,16	6,8,9,13	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	3,7,10,12,14,17	6,8,9,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,7,10,12,14,16,18	6,8,9,13,15,18	2^{-12}

Table 0.320 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	3,7,10,17,18	6,8,9,11,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	3,7,10,16	6,8,9,11	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	3,7,10,17	6,8,9,11,15,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	3,7,10,16,18	6,8,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	3,7,10,14	6,8,9,11	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	3,7,10,14,16,17,18	6,8,9,11,17,18	2^{-1}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	3,7,10,14,18	6,8,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	3,7,10,14,16,17	6,8,9,11,15,17	2^{-1}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	3,7,10,17	6,8,9,11,13,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	3,7,10,16,18	6,8,9,11,13,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	3,7,10,17,18	6,8,9,11,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	3,7,10,16	6,8,9,11,13,15	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	3,7,10,14,18	6,8,9,11,13,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	3,7,10,14,16,17	6,8,9,11,13,17	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	3,7,10,14	6,8,9,11,13,15	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	3,7,10,14,16,17,18	6,8,9,11,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	3,7,10,12	6,8,9,11	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	3,7,10,12,16,17,18	6,8,9,11,17,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	3,7,10,12,18	6,8,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	3,7,10,12,16,17	6,8,9,11,15,17	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	3,7,10,12,14,17,18	6,8,9,11,17,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	3,7,10,12,14,16	6,8,9,11	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,7,10,12,14,17	6,8,9,11,15,17	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	3,7,10,12,14,16,18	6,8,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	3,7,10,12,18	6,8,9,11,13,18	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	3,7,10,12,16,17	6,8,9,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	3,7,10,12	6,8,9,11,13,15	2^{-23}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	3,7,10,12,16,17,18	6,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	3,7,10,12,14,17	6,8,9,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	3,7,10,12,14,16,18	6,8,9,11,13,18	2^{-12}
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	3,7,10,12,14,17,18	6,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	3,7,10,12,14,16	6,8,9,11,13,15	2^{-12}

Table 0.321 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	3,5	—	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	3,5,16,17,18	17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	3,5,18	15,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	3,5,16,17	15,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	3,5,14,17,18	17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	3,5,14,16	—	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	3,5,14,17	15,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	3,5,14,16,18	15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	3,5,18	13,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	3,5,16,17	13,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	3,5	13,15	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	3,5,16,17,18	13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	3,5,14,17	13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	3,5,14,16,18	13,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	3,5,14,17,18	13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	3,5,14,16	13,15	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	3,5,12,17,18	17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	3,5,12,16	—	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	3,5,12,17	15,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	3,5,12,16,18	15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	3,5,12,14	—	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	3,5,12,14,16,17,18	17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	3,5,12,14,18	15,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	3,5,12,14,16,17	15,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	3,5,12,17	13,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	3,5,12,16,18	13,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	3,5,12,17,18	13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	3,5,12,16	13,15	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	3,5,12,14,18	13,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	3,5,12,14,16,17	13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	3,5,12,14	13,15	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	3,5,12,14,16,17,18	13,15,17,18	$2^{-17.5}$

Table 0.322 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	3,5,18	11,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	3,5,16,17	11,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	3,5	11,15	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	3,5,16,17,18	11,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	3,5,14,17	11,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	3,5,14,16,18	11,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	3,5,14,17,18	11,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	3,5,14,16	11,15	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	3,5	11,13	2^{-1}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	3,5,16,17,18	11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	3,5,18	11,13,15,18	2^{-1}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	3,5,16,17	11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	3,5,14,17,18	11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	3,5,14,16	11,13	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	3,5,14,17	11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	3,5,14,16,18	11,13,15,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	3,5,12,17	11,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,12,16,18	11,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	3,5,12,17,18	11,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,12,16	11,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	3,5,12,14,18	11,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	3,5,12,14,16,17	11,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	3,5,12,14	11,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	3,5,12,14,16,17,18	11,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	3,5,12,17,18	11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	3,5,12,16	11,13	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	3,5,12,17	11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	3,5,12,16,18	11,13,15,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	3,5,12,14	11,13	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	3,5,12,14,16,17,18	11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	3,5,12,14,18	11,13,15,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	3,5,12,14,16,17	11,13,15,17	$2^{-17.5}$

Table 0.323 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	3,5,10,17,18	17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	3,5,10,16	—	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	3,5,10,17	15,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	3,5,10,16,18	15,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	3,5,10,14	—	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	3,5,10,14,16,17,18	17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	3,5,10,14,18	15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	3,5,10,14,16,17	15,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	3,5,10,17	13,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	3,5,10,16,18	13,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	3,5,10,17,18	13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	3,5,10,16	13,15	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	3,5,10,14,18	13,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	3,5,10,14,16,17	13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	3,5,10,14	13,15	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	3,5,10,14,16,17,18	13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	3,5,10,12	—	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	3,5,10,12,16,17,18	17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	3,5,10,12,18	15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	3,5,10,12,16,17	15,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	3,5,10,12,14,17,18	17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	3,5,10,12,14,16	—	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	3,5,10,12,14,17	15,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	3,5,10,12,14,16,18	15,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	3,5,10,12,18	13,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	3,5,10,12,16,17	13,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	3,5,10,12	13,15	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	3,5,10,12,16,17,18	13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,10,12,14,17	13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	3,5,10,12,14,16,18	13,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,10,12,14,17,18	13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	3,5,10,12,14,16	13,15	2^{-23}

Table 0.324 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,10,17	11,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	3,5,10,16,18	11,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,10,17,18	11,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	3,5,10,16	11,15	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	3,5,10,14,18	11,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5,10,14,16,17	11,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	3,5,10,14	11,15	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5,10,14,16,17,18	11,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,5,10,17,18	11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,5,10,16	11,13	2^{-34}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	3,5,10,17	11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	3,5,10,16,18	11,13,15,18	2^{-34}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	3,5,10,14	11,13	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	3,5,10,14,16,17,18	11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	3,5,10,14,18	11,13,15,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	3,5,10,14,16,17	11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	3,5,10,12,18	11,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	3,5,10,12,16,17	11,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	3,5,10,12	11,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	3,5,10,12,16,17,18	11,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	3,5,10,12,14,17	11,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	3,5,10,12,14,16,18	11,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	3,5,10,12,14,17,18	11,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	3,5,10,12,14,16	11,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	3,5,10,12	11,13	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	3,5,10,12,16,17,18	11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	3,5,10,12,18	11,13,15,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	3,5,10,12,16,17	11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	3,5,10,12,14,17,18	11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	3,5,10,12,14,16	11,13	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	3,5,10,12,14,17	11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	3,5,10,12,14,16,18	11,13,15,18	2^{-23}

Table 0.325 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	3,5,18	9,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	3,5,16,17	9,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	3,5	9,15	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	3,5,16,17,18	9,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	3,5,14,17	9,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	3,5,14,16,18	9,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	3,5,14,17,18	9,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	3,5,14,16	9,15	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	3,5	9,13	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,16,17,18	9,13,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	3,5,18	9,13,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,16,17	9,13,15,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	3,5,14,17,18	9,13,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	3,5,14,16	9,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	3,5,14,17	9,13,15,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	3,5,14,16,18	9,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	3,5,12,17	9,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	3,5,12,16,18	9,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	3,5,12,17,18	9,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	3,5,12,16	9,15	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	3,5,12,14,18	9,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,5,12,14,16,17	9,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	3,5,12,14	9,15	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	3,5,12,14,16,17,18	9,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	3,5,12,17,18	9,13,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	3,5,12,16	9,13	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	3,5,12,17	9,13,15,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	3,5,12,16,18	9,13,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	3,5,12,14	9,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	3,5,12,14,16,17,18	9,13,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	3,5,12,14,18	9,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	3,5,12,14,16,17	9,13,15,17	2^{-23}

Table 0.326 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	3,5	9,11	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	3,5,16,17,18	9,11,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	3,5,18	9,11,15,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	3,5,16,17	9,11,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	3,5,14,17,18	9,11,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	3,5,14,16	9,11	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	3,5,14,17	9,11,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	3,5,14,16,18	9,11,15,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	3,5,18	9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	3,5,16,17	9,11,13,17	2^{-34}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	3,5	9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	3,5,16,17,18	9,11,13,15,17,18	2^{-34}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	3,5,14,17	9,11,13,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	3,5,14,16,18	9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	3,5,14,17,18	9,11,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	3,5,14,16	9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	3,5,12,17,18	9,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	3,5,12,16	9,11	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	3,5,12,17	9,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	3,5,12,16,18	9,11,15,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	3,5,12,14	9,11	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	3,5,12,14,16,17,18	9,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	3,5,12,14,18	9,11,15,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	3,5,12,14,16,17	9,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	3,5,12,17	9,11,13,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	3,5,12,16,18	9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	3,5,12,17,18	9,11,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	3,5,12,16	9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	3,5,12,14,18	9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	3,5,12,14,16,17	9,11,13,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	3,5,12,14	9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	3,5,12,14,16,17,18	9,11,13,15,17,18	2^{-23}

Table 0.327 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	3,5,10,17	9,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	3,5,10,16,18	9,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	3,5,10,17,18	9,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	3,5,10,16	9,15	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	3,5,10,14,18	9,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	3,5,10,14,16,17	9,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	3,5,10,14	9,15	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	3,5,10,14,16,17,18	9,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,10,17,18	9,13,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	3,5,10,16	9,13	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,10,17	9,13,15,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	3,5,10,16,18	9,13,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	3,5,10,14	9,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	3,5,10,14,16,17,18	9,13,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	3,5,10,14,18	9,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	3,5,10,14,16,17	9,13,15,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	3,5,10,12,18	9,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	3,5,10,12,16,17	9,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	3,5,10,12	9,15	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	3,5,10,12,16,17,18	9,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	3,5,10,12,14,17	9,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	3,5,10,12,14,16,18	9,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	3,5,10,12,14,17,18	9,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	3,5,10,12,14,16	9,15	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	3,5,10,12	9,13	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	3,5,10,12,16,17,18	9,13,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	3,5,10,12,18	9,13,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	3,5,10,12,16,17	9,13,15,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	3,5,10,12,14,17,18	9,13,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	3,5,10,12,14,16	9,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	3,5,10,12,14,17	9,13,15,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	3,5,10,12,14,16,18	9,13,15,18	$2^{-17.5}$

Table 0.328 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	3,5,10,17,18	9,11,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	3,5,10,16	9,11	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	3,5,10,17	9,11,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	3,5,10,16,18	9,11,15,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	3,5,10,14	9,11	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	3,5,10,14,16,17,18	9,11,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	3,5,10,14,18	9,11,15,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	3,5,10,14,16,17	9,11,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	3,5,10,17	9,11,13,17	2^{-1}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	3,5,10,16,18	9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	3,5,10,17,18	9,11,13,15,17,18	2^{-1}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	3,5,10,16	9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	3,5,10,14,18	9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	3,5,10,14,16,17	9,11,13,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	3,5,10,14	9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	3,5,10,14,16,17,18	9,11,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	3,5,10,12	9,11	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	3,5,10,12,16,17,18	9,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	3,5,10,12,18	9,11,15,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	3,5,10,12,16,17	9,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	3,5,10,12,14,17,18	9,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	3,5,10,12,14,16	9,11	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	3,5,10,12,14,17	9,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	3,5,10,12,14,16,18	9,11,15,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	3,5,10,12,18	9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	3,5,10,12,16,17	9,11,13,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	3,5,10,12	9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,5,10,12,16,17,18	9,11,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	3,5,10,12,14,17	9,11,13,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5,10,12,14,16,18	9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	3,5,10,12,14,17,18	9,11,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,5,10,12,14,16	9,11,13,15	$2^{-17.5}$

Table 0.329 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	3,5,17,18	8,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	3,5,16	8	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	3,5,17	8,15,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	3,5,16,18	8,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	3,5,14	8	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	3,5,14,16,17,18	8,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	3,5,14,18	8,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	3,5,14,16,17	8,15,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	3,5,17	8,13,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,16,18	8,13,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	3,5,17,18	8,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,16	8,13,15	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	3,5,14,18	8,13,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	3,5,14,16,17	8,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	3,5,14	8,13,15	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	3,5,14,16,17,18	8,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	3,5,12	8	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	3,5,12,16,17,18	8,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	3,5,12,18	8,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	3,5,12,16,17	8,15,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	3,5,12,14,17,18	8,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	3,5,12,14,16	8	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	3,5,12,14,17	8,15,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	3,5,12,14,16,18	8,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	3,5,12,18	8,13,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	3,5,12,16,17	8,13,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	3,5,12	8,13,15	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	3,5,12,16,17,18	8,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	3,5,12,14,17	8,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	3,5,12,14,16,18	8,13,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	3,5,12,14,17,18	8,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	3,5,12,14,16	8,13,15	2^{-12}

Table 0.330 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,17	8,11,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	3,5,16,18	8,11,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	3,5,17,18	8,11,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	3,5,16	8,11,15	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	3,5,14,18	8,11,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	3,5,14,16,17	8,11,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	3,5,14	8,11,15	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	3,5,14,16,17,18	8,11,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	3,5,17,18	8,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	3,5,16	8,11,13	2^{-1}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	3,5,17	8,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	3,5,16,18	8,11,13,15,18	2^{-1}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	3,5,14	8,11,13	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	3,5,14,16,17,18	8,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	3,5,14,18	8,11,13,15,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	3,5,14,16,17	8,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	3,5,12,18	8,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	3,5,12,16,17	8,11,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	3,5,12	8,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	3,5,12,16,17,18	8,11,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	3,5,12,14,17	8,11,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	3,5,12,14,16,18	8,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	3,5,12,14,17,18	8,11,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	3,5,12,14,16	8,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	3,5,12	8,11,13	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	3,5,12,16,17,18	8,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	3,5,12,18	8,11,13,15,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	3,5,12,16,17	8,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	3,5,12,14,17,18	8,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	3,5,12,14,16	8,11,13	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	3,5,12,14,17	8,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	3,5,12,14,16,18	8,11,13,15,18	2^{-12}

Table 0.331 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	3,5,10	8	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	3,5,10,16,17,18	8,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	3,5,10,18	8,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	3,5,10,16,17	8,15,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	3,5,10,14,17,18	8,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	3,5,10,14,16	8	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	3,5,10,14,17	8,15,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	3,5,10,14,16,18	8,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,10,18	8,13,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	3,5,10,16,17	8,13,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,10	8,13,15	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	3,5,10,16,17,18	8,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	3,5,10,14,17	8,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	3,5,10,14,16,18	8,13,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	3,5,10,14,17,18	8,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	3,5,10,14,16	8,13,15	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	3,5,10,12,17,18	8,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	3,5,10,12,16	8	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	3,5,10,12,17	8,15,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	3,5,10,12,16,18	8,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	3,5,10,12,14	8	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	3,5,10,12,14,16,17,18	8,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	3,5,10,12,14,18	8,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	3,5,10,12,14,16,17	8,15,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,5,10,12,17	8,13,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	3,5,10,12,16,18	8,13,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	3,5,10,12,17,18	8,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	3,5,10,12,16	8,13,15	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	3,5,10,12,14,18	8,13,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	3,5,10,12,14,16,17	8,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	3,5,10,12,14	8,13,15	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	3,5,10,12,14,16,17,18	8,13,15,17,18	$2^{-17.5}$

Table 0.332 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	3,5,10,18	8,11,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	3,5,10,16,17	8,11,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	3,5,10	8,11,15	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	3,5,10,16,17,18	8,11,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	3,5,10,14,17	8,11,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	3,5,10,14,16,18	8,11,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	3,5,10,14,17,18	8,11,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	3,5,10,14,16	8,11,15	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	3,5,10	8,11,13	2^{-34}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	3,5,10,16,17,18	8,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	3,5,10,18	8,11,13,15,18	2^{-34}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	3,5,10,16,17	8,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	3,5,10,14,17,18	8,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	3,5,10,14,16	8,11,13	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	3,5,10,14,17	8,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	3,5,10,14,16,18	8,11,13,15,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	3,5,10,12,17	8,11,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	3,5,10,12,16,18	8,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	3,5,10,12,17,18	8,11,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	3,5,10,12,16	8,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	3,5,10,12,14,18	8,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	3,5,10,12,14,16,17	8,11,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	3,5,10,12,14	8,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	3,5,10,12,14,16,17,18	8,11,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	3,5,10,12,17,18	8,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	3,5,10,12,16	8,11,13	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	3,5,10,12,17	8,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	3,5,10,12,16,18	8,11,13,15,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	3,5,10,12,14	8,11,13	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	3,5,10,12,14,16,17,18	8,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	3,5,10,12,14,18	8,11,13,15,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	3,5,10,12,14,16,17	8,11,13,15,17	$2^{-17.5}$

Table 0.333 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	3,5,17	8,9,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	3,5,16,18	8,9,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	3,5,17,18	8,9,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	3,5,16	8,9,15	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	3,5,14,18	8,9,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	3,5,14,16,17	8,9,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	3,5,14	8,9,15	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	3,5,14,16,17,18	8,9,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	3,5,17,18	8,9,13,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	3,5,16	8,9,13	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	3,5,17	8,9,13,15,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	3,5,16,18	8,9,13,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	3,5,14	8,9,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	3,5,14,16,17,18	8,9,13,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	3,5,14,18	8,9,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	3,5,14,16,17	8,9,13,15,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	3,5,12,18	8,9,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	3,5,12,16,17	8,9,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	3,5,12	8,9,15	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	3,5,12,16,17,18	8,9,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	3,5,12,14,17	8,9,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	3,5,12,14,16,18	8,9,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	3,5,12,14,17,18	8,9,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	3,5,12,14,16	8,9,15	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	3,5,12	8,9,13	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	3,5,12,16,17,18	8,9,13,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	3,5,12,18	8,9,13,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	3,5,12,16,17	8,9,13,15,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	3,5,12,14,17,18	8,9,13,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,12,14,16	8,9,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	3,5,12,14,17	8,9,13,15,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,12,14,16,18	8,9,13,15,18	$2^{-17.5}$

Table 0.334 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	3,5,17,18	8,9,11,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,16	8,9,11	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	3,5,17	8,9,11,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,16,18	8,9,11,15,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5,14	8,9,11	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	3,5,14,16,17,18	8,9,11,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5,14,18	8,9,11,15,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	3,5,14,16,17	8,9,11,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,5,17	8,9,11,13,17	2^{-34}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,5,16,18	8,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	3,5,17,18	8,9,11,13,15,17,18	2^{-34}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	3,5,16	8,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	3,5,14,18	8,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	3,5,14,16,17	8,9,11,13,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	3,5,14	8,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	3,5,14,16,17,18	8,9,11,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	3,5,12	8,9,11	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	3,5,12,16,17,18	8,9,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	3,5,12,18	8,9,11,15,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	3,5,12,16,17	8,9,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	3,5,12,14,17,18	8,9,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	3,5,12,14,16	8,9,11	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	3,5,12,14,17	8,9,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	3,5,12,14,16,18	8,9,11,15,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	3,5,12,18	8,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	3,5,12,16,17	8,9,11,13,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	3,5,12	8,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	3,5,12,16,17,18	8,9,11,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	3,5,12,14,17	8,9,11,13,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	3,5,12,14,16,18	8,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	3,5,12,14,17,18	8,9,11,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	3,5,12,14,16	8,9,11,13,15	$2^{-17.5}$

Table 0.335 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	3,5,10,18	8,9,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	3,5,10,16,17	8,9,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	3,5,10	8,9,15	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	3,5,10,16,17,18	8,9,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	3,5,10,14,17	8,9,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	3,5,10,14,16,18	8,9,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	3,5,10,14,17,18	8,9,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	3,5,10,14,16	8,9,15	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	3,5,10	8,9,13	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	3,5,10,16,17,18	8,9,13,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	3,5,10,18	8,9,13,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	3,5,10,16,17	8,9,13,15,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	3,5,10,14,17,18	8,9,13,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	3,5,10,14,16	8,9,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	3,5,10,14,17	8,9,13,15,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	3,5,10,14,16,18	8,9,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	3,5,10,12,17	8,9,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	3,5,10,12,16,18	8,9,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	3,5,10,12,17,18	8,9,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	3,5,10,12,16	8,9,15	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	3,5,10,12,14,18	8,9,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	3,5,10,12,17,18	8,9,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	3,5,10,12,14,16,17	8,9,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	3,5,10,12,14	8,9,15	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	3,5,10,12,14,16,17,18	8,9,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	3,5,10,12,17,18	8,9,13,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	3,5,10,12,16	8,9,13	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	3,5,10,12,17	8,9,13,15,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	3,5,10,12,16,18	8,9,13,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	3,5,10,12,14	8,9,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	3,5,10,12,14,16,17,18	8,9,13,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	3,5,10,12,14,18	8,9,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	3,5,10,12,14,16,17	8,9,13,15,17	2^{-12}

Table 0.336 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	3,5,10	8,9,11	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	3,5,10,16,17,18	8,9,11,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	3,5,10,18	8,9,11,15,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	3,5,10,16,17	8,9,11,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	3,5,10,14,17,18	8,9,11,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	3,5,10,14,16	8,9,11	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	3,5,10,14,17	8,9,11,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	3,5,10,14,16,18	8,9,11,15,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	3,5,10,18	8,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	3,5,10,16,17	8,9,11,13,17	2^{-1}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	3,5,10	8,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	3,5,10,16,17,18	8,9,11,13,15,17,18	2^{-1}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	3,5,10,14,17	8,9,11,13,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	3,5,10,14,16,18	8,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	3,5,10,14,17,18	8,9,11,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	3,5,10,14,16	8,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,10,12,17,18	8,9,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	3,5,10,12,16	8,9,11	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,10,12,17	8,9,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	3,5,10,12,16,18	8,9,11,15,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	3,5,10,12,14	8,9,11	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	3,5,10,12,14,16,17,18	8,9,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	3,5,10,12,14,18	8,9,11,15,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	3,5,10,12,14,16,17	8,9,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	3,5,10,12,17	8,9,11,13,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	3,5,10,12,16,18	8,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	3,5,10,12,17,18	8,9,11,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	3,5,10,12,16	8,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	3,5,10,12,14,18	8,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	3,5,10,12,14,16,17	8,9,11,13,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	3,5,10,12,14	8,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	3,5,10,12,14,16,17,18	8,9,11,13,15,17,18	2^{-12}

Table 0.337 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	3,5,7,18	18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	3,5,7,16,17	17	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	3,5,7	15	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	3,5,7,16,17,18	15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	3,5,7,14,17	17	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	3,5,7,14,16,18	18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	3,5,7,14,17,18	15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	3,5,7,14,16	15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	3,5,7	13	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	3,5,7,16,17,18	13,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	3,5,7,18	13,15,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	3,5,7,16,17	13,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	3,5,7,14,17,18	13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	3,5,7,14,16	13	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	3,5,7,14,17	13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	3,5,7,14,16,18	13,15,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	3,5,7,12,17	17	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	3,5,7,12,16,18	18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	3,5,7,12,17,18	15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	3,5,7,12,16	15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	3,5,7,12,14,18	18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	3,5,7,12,14,16,17	17	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	3,5,7,12,14	15	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	3,5,7,12,14,16,17,18	15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	3,5,7,12,17,18	13,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	3,5,7,12,16	13	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	3,5,7,12,17	13,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	3,5,7,12,16,18	13,15,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	3,5,7,12,14	13	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	3,5,7,12,14,16,17,18	13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	3,5,7,12,14,18	13,15,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	3,5,7,12,14,16,17	13,15,17	$2^{-17.5}$

Table 0.338 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	3,5,7	11	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	3,5,7,16,17,18	11,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	3,5,7,18	11,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	3,5,7,16,17	11,15,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	3,5,7,14,17,18	11,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	3,5,7,14,16	11	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	3,5,7,14,17	11,15,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	3,5,7,14,16,18	11,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	3,5,7,18	11,13,18	2^{-1}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,7,16,17	11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	3,5,7	11,13,15	2^{-1}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,7,16,17,18	11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	3,5,7,14,17	11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	3,5,7,14,16,18	11,13,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	3,5,7,14,17,18	11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	3,5,7,14,16	11,13,15	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	3,5,7,12,17,18	11,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	3,5,7,12,16	11	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	3,5,7,12,17	11,15,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	3,5,7,12,16,18	11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	3,5,7,12,14	11	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	3,5,7,12,14,16,17,18	11,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	3,5,7,12,14,18	11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	3,5,7,12,14,16,17	11,15,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	3,5,7,12,17	11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	3,5,7,12,16,18	11,13,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	3,5,7,12,17,18	11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	3,5,7,12,16	11,13,15	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	3,5,7,12,14,18	11,13,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	3,5,7,12,14,16,17	11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	3,5,7,12,14	11,13,15	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	3,5,7,12,14,16,17,18	11,13,15,17,18	$2^{-17.5}$

Table 0.339 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	3,5,7,10,17	17	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	3,5,7,10,16,18	18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	3,5,7,10,17,18	15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	3,5,7,10,16	15	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	3,5,7,10,14,18	18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	3,5,7,10,14,16,17	17	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	3,5,7,10,14	15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	3,5,7,10,14,16,17,18	15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	3,5,7,10,17,18	13,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	3,5,7,10,16	13	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	3,5,7,10,17	13,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	3,5,7,10,16,18	13,15,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	3,5,7,10,14	13	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	3,5,7,10,14,16,17,18	13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	3,5,7,10,14,18	13,15,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	3,5,7,10,14,16,17	13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	3,5,7,10,12,18	18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	3,5,7,10,12,16,17	17	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	3,5,7,10,12	15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	3,5,7,10,12,16,17,18	15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	3,5,7,10,12,14,17	17	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	3,5,7,10,12,14,16,18	18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	3,5,7,10,12,14,16	15	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	3,5,7,10,12	13	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	3,5,7,10,12,16,17,18	13,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	3,5,7,10,12,18	13,15,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	3,5,7,10,12,16,17	13,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	3,5,7,10,12,14,17,18	13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	3,5,7,10,12,14,16	13	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	3,5,7,10,12,14,17	13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	3,5,7,10,12,14,16,18	13,15,18	2^{-23}

Table 0.340 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	3,5,7,10,17,18	11,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	3,5,7,10,16	11	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	3,5,7,10,17	11,15,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	3,5,7,10,16,18	11,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	3,5,7,10,14	11	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	3,5,7,10,14,16,17,18	11,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	3,5,7,10,14,18	11,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	3,5,7,10,14,16,17	11,15,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,7,10,17	11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	3,5,7,10,16,18	11,13,18	2^{-34}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,7,10,17,18	11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	3,5,7,10,16	11,13,15	2^{-34}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	3,5,7,10,14,18	11,13,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	3,5,7,10,14,16,17	11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	3,5,7,10,14	11,13,15	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	3,5,7,10,14,16,17,18	11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	3,5,7,10,12	11	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	3,5,7,10,12,16,17,18	11,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	3,5,7,10,12,18	11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	3,5,7,10,12,16,17	11,15,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	3,5,7,10,12,14,17,18	11,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	3,5,7,10,12,14,16	11	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	3,5,7,10,12,14,17	11,15,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	3,5,7,10,12,14,16,18	11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	3,5,7,10,12,18	11,13,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	3,5,7,10,12,16,17	11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	3,5,7,10,12	11,13,15	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	3,5,7,10,12,16,17,18	11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	3,5,7,10,12,14,17	11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	3,5,7,10,12,14,16,18	11,13,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	3,5,7,10,12,14,17,18	11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	3,5,7,10,12,14,16	11,13,15	2^{-23}

Table 0.341 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	3,5,7	9	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	3,5,7,16,17,18	9,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	3,5,7,18	9,15,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	3,5,7,16,17	9,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	3,5,7,14,17,18	9,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	3,5,7,14,16	9	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	3,5,7,14,17	9,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	3,5,7,14,16,18	9,15,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	3,5,7,18	9,13,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	3,5,7,16,17	9,13,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	3,5,7	9,13,15	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	3,5,7,16,17,18	9,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	3,5,7,14,17	9,13,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	3,5,7,14,16,18	9,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	3,5,7,14,17,18	9,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	3,5,7,14,16	9,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	3,5,7,12,17,18	9,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,12,16	9	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	3,5,7,12,17	9,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,12,16,18	9,15,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,12,14	9	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	3,5,7,12,14,16,17,18	9,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,12,14,18	9,15,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	3,5,7,12,14,16,17	9,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	3,5,7,12,17	9,13,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	3,5,7,12,16,18	9,13,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	3,5,7,12,17,18	9,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	3,5,7,12,16	9,13,15	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	3,5,7,12,14,18	9,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	3,5,7,12,14,16,17	9,13,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	3,5,7,12,14	9,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5,7,12,14,16,17,18	9,13,15,17,18	2^{-23}

Table 0.342 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	3,5,7,18	9,11,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	3,5,7,16,17	9,11,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	3,5,7	9,11,15	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	3,5,7,16,17,18	9,11,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	3,5,7,14,17	9,11,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	3,5,7,14,16,18	9,11,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	3,5,7,14,17,18	9,11,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	3,5,7,14,16	9,11,15	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	3,5,7	9,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	3,5,7,16,17,18	9,11,13,17,18	2^{-34}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	3,5,7,18	9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	3,5,7,16,17	9,11,13,15,17	2^{-34}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	3,5,7,14,17,18	9,11,13,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	3,5,7,14,16	9,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	3,5,7,14,17	9,11,13,15,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	3,5,7,14,16,18	9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	3,5,7,12,17	9,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	3,5,7,12,16,18	9,11,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	3,5,7,12,17,18	9,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	3,5,7,12,16	9,11,15	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	3,5,7,12,14,18	9,11,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	3,5,7,12,14,16,17	9,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	3,5,7,12,14	9,11,15	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	3,5,7,12,14,16,17,18	9,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	3,5,7,12,17,18	9,11,13,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	3,5,7,12,16	9,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	3,5,7,12,17	9,11,13,15,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	3,5,7,12,16,18	9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	3,5,7,12,14	9,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	3,5,7,12,14,16,17,18	9,11,13,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	3,5,7,12,14,18	9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	3,5,7,12,14,16,17	9,11,13,15,17	2^{-23}

Table 0.343 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,10,17,18	9,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	3,5,7,10,16	9	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	3,5,7,10,17	9,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	3,5,7,10,16,18	9,15,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	3,5,7,10,14	9	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5,7,10,14,16,17,18	9,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	3,5,7,10,14,18	9,15,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5,7,10,14,16,17	9,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	3,5,7,10,17	9,13,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	3,5,7,10,16,18	9,13,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,5,7,10,17,18	9,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,5,7,10,16	9,13,15	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	3,5,7,10,14,18	9,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	3,5,7,10,14,16,17	9,13,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	3,5,7,10,14	9,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	3,5,7,10,14,16,17,18	9,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,10,12	9	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	3,5,7,10,12,16,17,18	9,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	3,5,7,10,12,18	9,15,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	3,5,7,10,12,16,17	9,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	3,5,7,10,12,14,17,18	9,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	3,5,7,10,12,14,16	9	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	3,5,7,10,12,14,17	9,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	3,5,7,10,12,14,16,18	9,15,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	3,5,7,10,12,18	9,13,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	3,5,7,10,12,16,17	9,13,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	3,5,7,10,12	9,13,15	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	3,5,7,10,12,16,17,18	9,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	3,5,7,10,12,14,17	9,13,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	3,5,7,10,12,14,16,18	9,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	3,5,7,10,12,14,17,18	9,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	3,5,7,10,12,14,16	9,13,15	$2^{-17.5}$

Table 0.344 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	3,5,7,10,17	9,11,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	3,5,7,10,16,18	9,11,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	3,5,7,10,17,18	9,11,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	3,5,7,10,16	9,11,15	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	3,5,7,10,14,18	9,11,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	3,5,7,10,14,16,17	9,11,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	3,5,7,10,14	9,11,15	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	3,5,7,10,14,16,17,18	9,11,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	3,5,7,10,17,18	9,11,13,17,18	2^{-1}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	3,5,7,10,16	9,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	3,5,7,10,17	9,11,13,15,17	2^{-1}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	3,5,7,10,16,18	9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	3,5,7,10,14	9,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	3,5,7,10,14,16,17,18	9,11,13,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	3,5,7,10,14,18	9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	3,5,7,10,14,16,17	9,11,13,15,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	3,5,7,10,12,18	9,11,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	3,5,7,10,12,16,17	9,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	3,5,7,10,12	9,11,15	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	3,5,7,10,12,16,17,18	9,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	3,5,7,10,12,14,17	9,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	3,5,7,10,12,14,16,18	9,11,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	3,5,7,10,12,14,17,18	9,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	3,5,7,10,12,14,16	9,11,15	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	3,5,7,10,12	9,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	3,5,7,10,12,16,17,18	9,11,13,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	3,5,7,10,12,18	9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	3,5,7,10,12,16,17	9,11,13,15,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,7,10,12,14,17,18	9,11,13,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	3,5,7,10,12,14,16	9,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,7,10,12,14,17	9,11,13,15,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	3,5,7,10,12,14,16,18	9,11,13,15,18	$2^{-17.5}$

Table 0.345 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	3,5,7,17	8,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,16,18	8,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	3,5,7,17,18	8,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,16	8,15	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5,7,14,18	8,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	3,5,7,14,16,17	8,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5,7,14	8,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	3,5,7,14,16,17,18	8,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	3,5,7,17,18	8,13,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	3,5,7,16	8,13	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,5,7,17	8,13,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,5,7,16,18	8,13,15,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	3,5,7,14	8,13	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	3,5,7,14,16,17,18	8,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	3,5,7,14,18	8,13,15,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	3,5,7,14,16,17	8,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	3,5,7,12,18	8,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	3,5,7,12,16,17	8,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	3,5,7,12	8,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	3,5,7,12,16,17,18	8,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	3,5,7,12,14,17	8,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	3,5,7,12,14,16,18	8,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	3,5,7,12,14,17,18	8,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	3,5,7,12,14,16	8,15	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	3,5,7,12	8,13	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	3,5,7,12,16,17,18	8,13,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	3,5,7,12,18	8,13,15,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	3,5,7,12,16,17	8,13,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	3,5,7,12,14,17,18	8,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	3,5,7,12,14,16	8,13	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	3,5,7,12,14,17	8,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	3,5,7,12,14,16,18	8,13,15,18	2^{-12}

Table 0.346 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	3,5,7,17,18	8,11,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	3,5,7,16	8,11	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	3,5,7,17	8,11,15,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	3,5,7,16,18	8,11,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	3,5,7,14	8,11	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	3,5,7,14,16,17,18	8,11,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	3,5,7,14,18	8,11,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	3,5,7,14,16,17	8,11,15,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	3,5,7,17	8,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	3,5,7,16,18	8,11,13,18	2^{-1}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	3,5,7,17,18	8,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	3,5,7,16	8,11,13,15	2^{-1}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	3,5,7,14,18	8,11,13,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	3,5,7,14,16,17	8,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	3,5,7,14	8,11,13,15	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	3,5,7,14,16,17,18	8,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	3,5,7,12	8,11	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	3,5,7,12,16,17,18	8,11,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	3,5,7,12,18	8,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	3,5,7,12,16,17	8,11,15,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	3,5,7,12,14,17,18	8,11,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	3,5,7,12,14,16	8,11	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	3,5,7,12,14,17	8,11,15,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	3,5,7,12,14,16,18	8,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	3,5,7,12,18	8,11,13,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	3,5,7,12,16,17	8,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	3,5,7,12	8,11,13,15	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	3,5,7,12,16,17,18	8,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	3,5,7,12,14,17	8,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,7,12,14,16,18	8,11,13,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	3,5,7,12,14,17,18	8,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,7,12,14,16	8,11,13,15	2^{-12}

Table 0.347 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	3,5,7,10,18	8,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	3,5,7,10,16,17	8,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	3,5,7,10	8,15	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	3,5,7,10,16,17,18	8,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	3,5,7,10,14,17	8,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	3,5,7,10,14,16,18	8,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	3,5,7,10,14,17,18	8,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	3,5,7,10,14,16	8,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	3,5,7,10	8,13	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	3,5,7,10,16,17,18	8,13,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	3,5,7,10,18	8,13,15,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	3,5,7,10,16,17	8,13,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	3,5,7,10,14,17,18	8,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	3,5,7,10,14,16	8,13	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	3,5,7,10,14,17	8,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	3,5,7,10,14,16,18	8,13,15,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,10,12,17	8,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	3,5,7,10,12,16,18	8,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,10,12,17,18	8,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	3,5,7,10,12,16	8,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	3,5,7,10,12,14,18	8,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,10,12,14,16,17	8,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	3,5,7,10,12,14	8,15	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,10,12,14,16,17,18	8,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	3,5,7,10,12,17,18	8,13,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	3,5,7,10,12,16	8,13	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	3,5,7,10,12,17	8,13,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	3,5,7,10,12,16,18	8,13,15,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	3,5,7,10,12,14	8,13	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	3,5,7,10,12,14,16,17,18	8,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	3,5,7,10,12,14,18	8,13,15,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	3,5,7,10,12,14,16,17	8,13,15,17	$2^{-17.5}$

Table 0.348 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	3,5,7,10	8,11	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	3,5,7,10,16,17,18	8,11,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	3,5,7,10,18	8,11,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	3,5,7,10,16,17	8,11,15,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	3,5,7,10,14,17,18	8,11,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	3,5,7,10,14,16	8,11	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	3,5,7,10,14,17	8,11,15,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	3,5,7,10,14,16,18	8,11,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	3,5,7,10,18	8,11,13,18	2^{-34}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	3,5,7,10,16,17	8,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	3,5,7,10	8,11,13,15	2^{-34}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	3,5,7,10,16,17,18	8,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	3,5,7,10,14,17	8,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	3,5,7,10,14,16,18	8,11,13,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	3,5,7,10,14,17,18	8,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	3,5,7,10,14,16	8,11,13,15	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	3,5,7,10,12,17,18	8,11,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	3,5,7,10,12,16	8,11	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	3,5,7,10,12,17	8,11,15,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	3,5,7,10,12,16,18	8,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	3,5,7,10,12,14	8,11	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	3,5,7,10,12,14,16,17,18	8,11,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	3,5,7,10,12,14,18	8,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	3,5,7,10,12,14,16,17	8,11,15,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	3,5,7,10,12,17	8,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	3,5,7,10,12,16,18	8,11,13,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	3,5,7,10,12,17,18	8,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	3,5,7,10,12,16	8,11,13,15	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	3,5,7,10,12,14,18	8,11,13,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	3,5,7,10,12,14,16,17	8,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	3,5,7,10,12,14	8,11,13,15	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	3,5,7,10,12,14,16,17,18	8,11,13,15,17,18	$2^{-17.5}$

Table 0.349 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	3,5,7,17,18	8,9,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	3,5,7,16	8,9	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,7,17	8,9,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	3,5,7,16,18	8,9,15,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	3,5,7,14	8,9	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	3,5,7,14,16,17,18	8,9,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	3,5,7,14,18	8,9,15,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	3,5,7,14,16,17	8,9,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	3,5,7,17	8,9,13,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	3,5,7,16,18	8,9,13,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	3,5,7,17,18	8,9,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	3,5,7,16	8,9,13,15	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	3,5,7,14,18	8,9,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	3,5,7,14,16,17	8,9,13,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	3,5,7,14	8,9,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	3,5,7,14,16,17,18	8,9,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	3,5,7,12	8,9	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	3,5,7,12,16,17,18	8,9,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	3,5,7,12,18	8,9,15,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	3,5,7,12,16,17	8,9,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	3,5,7,12,14,17,18	8,9,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	3,5,7,12,14,16	8,9	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	3,5,7,12,14,17	8,9,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	3,5,7,12,14,16,18	8,9,15,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	3,5,7,12,18	8,9,13,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	3,5,7,12,16,17	8,9,13,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	3,5,7,12	8,9,13,15	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	3,5,7,12,16,17,18	8,9,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	3,5,7,12,14,17	8,9,13,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	3,5,7,12,14,16,18	8,9,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	3,5,7,12,14,17,18	8,9,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	3,5,7,12,14,16	8,9,13,15	$2^{-17.5}$

Table 0.350 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	3,5,7,17	8,9,11,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	3,5,7,16,18	8,9,11,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	3,5,7,17,18	8,9,11,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	3,5,7,16	8,9,11,15	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	3,5,7,14,18	8,9,11,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	3,5,7,14,16,17	8,9,11,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	3,5,7,14	8,9,11,15	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	3,5,7,14,16,17,18	8,9,11,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	3,5,7,17,18	8,9,11,13,17,18	2^{-34}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,7,16	8,9,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	3,5,7,17	8,9,11,13,15,17	2^{-34}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,7,16,18	8,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	3,5,7,14	8,9,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	3,5,7,14,16,17,18	8,9,11,13,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	3,5,7,14,18	8,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	3,5,7,14,16,17	8,9,11,13,15,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	3,5,7,12,18	8,9,11,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	3,5,7,12,16,17	8,9,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	3,5,7,12	8,9,11,15	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	3,5,7,12,16,17,18	8,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	3,5,7,12,14,17	8,9,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	3,5,7,12,14,16,18	8,9,11,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	3,5,7,12,14,17,18	8,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	3,5,7,12,14,16	8,9,11,15	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	3,5,7,12	8,9,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	3,5,7,12,16,17,18	8,9,11,13,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	3,5,7,12,18	8,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	3,5,7,12,16,17	8,9,11,13,15,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	3,5,7,12,14,17,18	8,9,11,13,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	3,5,7,12,14,16	8,9,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	3,5,7,12,14,17	8,9,11,13,15,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	3,5,7,12,14,16,18	8,9,11,13,15,18	$2^{-17.5}$

Table 0.351 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	3,5,7,10	8,9	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	3,5,7,10,16,17,18	8,9,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	3,5,7,10,18	8,9,15,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	3,5,7,10,16,17	8,9,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	3,5,7,10,14,17,18	8,9,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,7,10,14,16	8,9	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	3,5,7,10,14,17	8,9,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	3,5,7,10,14,16,18	8,9,15,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	3,5,7,10,18	8,9,13,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	3,5,7,10,16,17	8,9,13,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	3,5,7,10	8,9,13,15	$2^{-28.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	3,5,7,10,16,17,18	8,9,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	3,5,7,10,14,17	8,9,13,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	3,5,7,10,14,16,18	8,9,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	3,5,7,10,14,17,18	8,9,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	3,5,7,10,14,16	8,9,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	3,5,7,10,12,17,18	8,9,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	3,5,7,10,12,16	8,9	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	3,5,7,10,12,17	8,9,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	3,5,7,10,12,16,18	8,9,15,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	3,5,7,10,12,14	8,9	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	3,5,7,10,12,14,16,17,18	8,9,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	3,5,7,10,12,14,18	8,9,15,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	3,5,7,10,12,14,16,17	8,9,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	3,5,7,10,12,17	8,9,13,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	3,5,7,10,12,16,18	8,9,13,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	3,5,7,10,12,17,18	8,9,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	3,5,7,10,12,16	8,9,13,15	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	3,5,7,10,12,14,18	8,9,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	3,5,7,10,12,14,16,17	8,9,13,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	3,5,7,10,12,14	8,9,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	3,5,7,10,12,14,16,17,18	8,9,13,15,17,18	2^{-12}

Table 0.352 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	3,5,7,10,18	8,9,11,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	3,5,7,10,16,17	8,9,11,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	3,5,7,10	8,9,11,15	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	3,5,7,10,16,17,18	8,9,11,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	3,5,7,10,14,17	8,9,11,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	3,5,7,10,14,16,18	8,9,11,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	3,5,7,10,14,17,18	8,9,11,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	3,5,7,10,14,16	8,9,11,15	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,7,10	8,9,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	3,5,7,10,16,17,18	8,9,11,13,17,18	2^{-1}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,7,10,18	8,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	3,5,7,10,16,17	8,9,11,13,15,17	2^{-1}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	3,5,7,10,14,17,18	8,9,11,13,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	3,5,7,10,14,16	8,9,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	3,5,7,10,14,17	8,9,11,13,15,17	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	3,5,7,10,14,16,18	8,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	3,5,7,10,12,17	8,9,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	3,5,7,10,12,16,18	8,9,11,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	3,5,7,10,12,17,18	8,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	3,5,7,10,12,16	8,9,11,15	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	3,5,7,10,12,14,18	8,9,11,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	3,5,7,10,12,14,16,17	8,9,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	3,5,7,10,12,14	8,9,11,15	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	3,5,7,10,12,14,16,17,18	8,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	3,5,7,10,12,17,18	8,9,11,13,17,18	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	3,5,7,10,12,16	8,9,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	3,5,7,10,12,17	8,9,11,13,15,17	2^{-23}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	3,5,7,10,12,16,18	8,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	3,5,7,10,12,14	8,9,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	3,5,7,10,12,14,16,17,18	8,9,11,13,17,18	2^{-12}
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	3,5,7,10,12,14,18	8,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	3,5,7,10,12,14,16,17	8,9,11,13,15,17	2^{-12}

Table 0.353 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	3,5,17,18	6,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	3,5,16	6	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	3,5,17	6,15,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	3,5,16,18	6,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	3,5,14	6	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	3,5,14,16,17,18	6,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	3,5,14,18	6,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	3,5,14,16,17	6,15,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,17	6,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	3,5,16,18	6,13,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,17,18	6,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	3,5,16	6,13,15	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	3,5,14,18	6,13,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	3,5,14,16,17	6,13,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	3,5,14	6,13,15	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	3,5,14,16,17,18	6,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	3,5,12	6	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	3,5,12,16,17,18	6,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	3,5,12,18	6,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	3,5,12,16,17	6,15,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	3,5,12,14,17,18	6,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	3,5,12,14,16	6	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	3,5,12,14,17	6,15,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	3,5,12,14,16,18	6,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	3,5,12,18	6,13,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,12,16,17	6,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	3,5,12	6,13,15	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	3,5,12,16,17,18	6,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	3,5,12,14,17	6,13,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	3,5,12,14,16,18	6,13,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	3,5,12,14,17,18	6,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	3,5,12,14,16	6,13,15	2^{-12}

Table 0.354 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	3,5,17	6,11,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	3,5,16,18	6,11,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	3,5,17,18	6,11,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	3,5,16	6,11,15	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	3,5,14,18	6,11,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	3,5,14,16,17	6,11,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	3,5,14	6,11,15	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	3,5,14,16,17,18	6,11,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	3,5,17,18	6,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	3,5,16	6,11,13	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	3,5,17	6,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	3,5,16,18	6,11,13,15,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	3,5,14	6,11,13	2^{-1}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	3,5,14,16,17,18	6,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	3,5,14,18	6,11,13,15,18	2^{-1}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	3,5,14,16,17	6,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	3,5,12,18	6,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5,12,16,17	6,11,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	3,5,12	6,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5,12,16,17,18	6,11,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,12,14,17	6,11,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	3,5,12,14,16,18	6,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,12,14,17,18	6,11,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	3,5,12,14,16	6,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	3,5,12	6,11,13	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	3,5,12,16,17,18	6,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	3,5,12,18	6,11,13,15,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	3,5,12,16,17	6,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,12,14,17,18	6,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,5,12,14,16	6,11,13	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,12,14,17	6,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	3,5,12,14,16,18	6,11,13,15,18	2^{-23}

Table 0.355 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	3,5,10	6	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	3,5,10,16,17,18	6,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	3,5,10,18	6,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	3,5,10,16,17	6,15,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	3,5,10,14,17,18	6,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	3,5,10,14,16	6	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	3,5,10,14,17	6,15,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	3,5,10,14,16,18	6,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	3,5,10,18	6,13,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	3,5,10,16,17	6,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	3,5,10	6,13,15	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	3,5,10,16,17,18	6,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	3,5,10,14,17	6,13,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	3,5,10,14,16,18	6,13,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	3,5,10,14,17,18	6,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	3,5,10,14,16	6,13,15	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	3,5,10,12,17,18	6,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	3,5,10,12,16	6	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	3,5,10,12,17	6,15,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	3,5,10,12,16,18	6,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	3,5,10,12,14	6	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	3,5,10,12,14,16,17,18	6,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	3,5,10,12,14,18	6,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	3,5,10,12,14,16,17	6,15,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	3,5,10,12,17	6,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	3,5,10,12,16,18	6,13,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	3,5,10,12,17,18	6,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	3,5,10,12,16	6,13,15	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	3,5,10,12,14,18	6,13,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	3,5,10,12,14,16,17	6,13,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	3,5,10,12,14	6,13,15	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	3,5,10,12,14,16,17,18	6,13,15,17,18	$2^{-28.5}$

Table 0.356 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	3,5,10,18	6,11,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	3,5,10,16,17	6,11,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	3,5,10	6,11,15	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	3,5,10,16,17,18	6,11,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	3,5,10,14,17	6,11,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,10,14,16,18	6,11,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	3,5,10,14,17,18	6,11,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,10,14,16	6,11,15	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5,10	6,11,13	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	3,5,10,16,17,18	6,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5,10,18	6,11,13,15,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	3,5,10,16,17	6,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	3,5,10,14,17,18	6,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	3,5,10,14,16	6,11,13	2^{-34}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	3,5,10,14,17	6,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	3,5,10,14,16,18	6,11,13,15,18	2^{-34}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	3,5,10,12,17	6,11,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	3,5,10,12,16,18	6,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	3,5,10,12,17,18	6,11,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	3,5,10,12,16	6,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	3,5,10,12,14,18	6,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	3,5,10,12,14,16,17	6,11,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	3,5,10,12,14	6,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	3,5,10,12,14,16,17,18	6,11,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	3,5,10,12,17,18	6,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,10,12,16	6,11,13	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	3,5,10,12,17	6,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	3,5,10,12,16,18	6,11,13,15,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	3,5,10,12,14	6,11,13	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	3,5,10,12,14,16,17,18	6,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	3,5,10,12,14,18	6,11,13,15,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	3,5,10,12,14,16,17	6,11,13,15,17	$2^{-17.5}$

Table 0.357 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	3,5,17	6,9,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	3,5,16,18	6,9,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	3,5,17,18	6,9,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	3,5,16	6,9,15	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	3,5,14,18	6,9,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	3,5,14,16,17	6,9,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	3,5,14	6,9,15	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	3,5,14,16,17,18	6,9,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	3,5,17,18	6,9,13,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	3,5,16	6,9,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	3,5,17	6,9,13,15,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	3,5,16,18	6,9,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	3,5,14	6,9,13	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	3,5,14,16,17,18	6,9,13,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	3,5,14,18	6,9,13,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	3,5,14,16,17	6,9,13,15,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	3,5,12,18	6,9,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	3,5,12,16,17	6,9,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	3,5,12	6,9,15	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	3,5,12,16,17,18	6,9,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	3,5,12,14,17	6,9,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	3,5,12,14,16,18	6,9,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	3,5,12,14,17,18	6,9,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	3,5,12,14,16	6,9,15	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	3,5,12	6,9,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	3,5,12,16,17,18	6,9,13,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	3,5,12,18	6,9,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	3,5,12,16,17	6,9,13,15,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,12,14,17,18	6,9,13,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	3,5,12,14,16	6,9,13	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,12,14,17	6,9,13,15,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	3,5,12,14,16,18	6,9,13,15,18	$2^{-28.5}$

Table 0.358 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	3,5,17,18	6,9,11,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	3,5,16	6,9,11	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	3,5,17	6,9,11,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	3,5,16,18	6,9,11,15,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	3,5,14	6,9,11	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	3,5,14,16,17,18	6,9,11,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	3,5,14,18	6,9,11,15,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	3,5,14,16,17	6,9,11,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	3,5,17	6,9,11,13,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	3,5,16,18	6,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	3,5,17,18	6,9,11,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	3,5,16	6,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	3,5,14,18	6,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	3,5,14,16,17	6,9,11,13,17	2^{-34}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	3,5,14	6,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	3,5,14,16,17,18	6,9,11,13,15,17,18	2^{-34}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	3,5,12	6,9,11	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	3,5,12,16,17,18	6,9,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	3,5,12,18	6,9,11,15,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	3,5,12,16,17	6,9,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	3,5,12,14,17,18	6,9,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	3,5,12,14,16	6,9,11	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	3,5,12,14,17	6,9,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	3,5,12,14,16,18	6,9,11,15,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	3,5,12,18	6,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	3,5,12,16,17	6,9,11,13,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	3,5,12	6,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	3,5,12,16,17,18	6,9,11,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	3,5,12,14,17	6,9,11,13,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	3,5,12,14,16,18	6,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	3,5,12,14,17,18	6,9,11,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	3,5,12,14,16	6,9,11,13,15	$2^{-17.5}$

Table 0.359 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	3,5,10,18	6,9,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	3,5,10,16,17	6,9,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	3,5,10	6,9,15	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	3,5,10,16,17,18	6,9,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	3,5,10,14,17	6,9,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	3,5,10,14,16,18	6,9,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	3,5,10,14,17,18	6,9,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	3,5,10,14,16	6,9,15	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	3,5,10	6,9,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	3,5,10,16,17,18	6,9,13,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	3,5,10,18	6,9,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	3,5,10,16,17	6,9,13,15,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	3,5,10,14,17,18	6,9,13,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	3,5,10,14,16	6,9,13	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	3,5,10,14,17	6,9,13,15,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	3,5,10,14,16,18	6,9,13,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	3,5,10,12,17	6,9,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	3,5,10,12,16,18	6,9,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	3,5,10,12,17,18	6,9,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	3,5,10,12,16	6,9,15	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	3,5,10,12,14,18	6,9,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	3,5,10,12,14,16,17	6,9,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	3,5,10,12,14	6,9,15	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	3,5,10,12,14,16,17,18	6,9,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	3,5,10,12,17,18	6,9,13,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	3,5,10,12,16	6,9,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	3,5,10,12,17	6,9,13,15,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	3,5,10,12,16,18	6,9,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	3,5,10,12,14	6,9,13	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,10,12,14,16,17,18	6,9,13,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	3,5,10,12,14,18	6,9,13,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,10,12,14,16,17	6,9,13,15,17	2^{-12}

Table 0.360 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	3,5,10	6,9,11	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	3,5,10,16,17,18	6,9,11,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	3,5,10,18	6,9,11,15,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	3,5,10,16,17	6,9,11,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	3,5,10,14,17,18	6,9,11,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	3,5,10,14,16	6,9,11	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	3,5,10,14,17	6,9,11,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	3,5,10,14,16,18	6,9,11,15,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	3,5,10,18	6,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	3,5,10,16,17	6,9,11,13,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	3,5,10	6,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	3,5,10,16,17,18	6,9,11,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	3,5,10,14,17	6,9,11,13,17	2^{-1}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	3,5,10,14,16,18	6,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	3,5,10,14,17,18	6,9,11,13,15,17,18	2^{-1}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	3,5,10,14,16	6,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	3,5,10,12,17,18	6,9,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	3,5,10,12,16	6,9,11	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,10,12,17	6,9,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	3,5,10,12,16,18	6,9,11,15,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	3,5,10,12,14	6,9,11	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	3,5,10,12,14,16,17,18	6,9,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	3,5,10,12,14,18	6,9,11,15,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	3,5,10,12,14,16,17	6,9,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	3,5,10,12,17	6,9,11,13,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	3,5,10,12,16,18	6,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	3,5,10,12,17,18	6,9,11,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	3,5,10,12,16	6,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	3,5,10,12,14,18	6,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	3,5,10,12,14,16,17	6,9,11,13,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	3,5,10,12,14	6,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	3,5,10,12,14,16,17,18	6,9,11,13,15,17,18	2^{-23}

Table 0.361 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	3,5	6,8	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	3,5,16,17,18	6,8,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	3,5,18	6,8,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	3,5,16,17	6,8,15,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	3,5,14,17,18	6,8,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	3,5,14,16	6,8	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	3,5,14,17	6,8,15,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	3,5,14,16,18	6,8,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	3,5,18	6,8,13,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	3,5,16,17	6,8,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	3,5	6,8,13,15	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	3,5,16,17,18	6,8,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	3,5,14,17	6,8,13,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	3,5,14,16,18	6,8,13,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	3,5,14,17,18	6,8,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	3,5,14,16	6,8,13,15	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	3,5,12,17,18	6,8,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	3,5,12,16	6,8	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	3,5,12,17	6,8,15,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	3,5,12,16,18	6,8,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	3,5,12,14	6,8	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	3,5,12,14,16,17,18	6,8,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	3,5,12,14,18	6,8,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	3,5,12,14,16,17	6,8,15,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	3,5,12,17	6,8,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	3,5,12,16,18	6,8,13,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	3,5,12,17,18	6,8,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	3,5,12,16	6,8,13,15	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,12,14,18	6,8,13,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	3,5,12,14,16,17	6,8,13,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,12,14	6,8,13,15	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	3,5,12,14,16,17,18	6,8,13,15,17,18	$2^{-6.5}$

Table 0.362 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	3,5,18	6,8,11,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,16,17	6,8,11,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	3,5	6,8,11,15	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,16,17,18	6,8,11,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	3,5,14,17	6,8,11,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	3,5,14,16,18	6,8,11,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	3,5,14,17,18	6,8,11,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	3,5,14,16	6,8,11,15	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	3,5	6,8,11,13	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	3,5,16,17,18	6,8,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	3,5,18	6,8,11,13,15,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	3,5,16,17	6,8,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	3,5,14,17,18	6,8,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	3,5,14,16	6,8,11,13	2^{-1}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	3,5,14,17	6,8,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	3,5,14,16,18	6,8,11,13,15,18	2^{-1}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	3,5,12,17	6,8,11,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,12,16,18	6,8,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	3,5,12,17,18	6,8,11,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,12,16	6,8,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	3,5,12,14,18	6,8,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	3,5,12,14,16,17	6,8,11,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	3,5,12,14	6,8,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	3,5,12,14,16,17,18	6,8,11,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,12,17,18	6,8,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	3,5,12,16	6,8,11,13	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,12,17	6,8,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	3,5,12,16,18	6,8,11,13,15,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	3,5,12,14	6,8,11,13	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	3,5,12,14,16,17,18	6,8,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	3,5,12,14,18	6,8,11,13,15,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	3,5,12,14,16,17	6,8,11,13,15,17	$2^{-17.5}$

Table 0.363 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	3,5,10,17,18	6,8,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	3,5,10,16	6,8	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	3,5,10,17	6,8,15,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	3,5,10,16,18	6,8,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	3,5,10,14	6,8	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	3,5,10,14,16,17,18	6,8,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	3,5,10,14,18	6,8,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	3,5,10,14,16,17	6,8,15,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	3,5,10,17	6,8,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	3,5,10,16,18	6,8,13,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	3,5,10,17,18	6,8,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	3,5,10,16	6,8,13,15	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	3,5,10,14,18	6,8,13,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	3,5,10,14,16,17	6,8,13,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	3,5,10,14	6,8,13,15	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	3,5,10,14,16,17,18	6,8,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	3,5,10,12	6,8	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	3,5,10,12,16,17,18	6,8,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	3,5,10,12,18	6,8,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	3,5,10,12,16,17	6,8,15,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	3,5,10,12,14,17,18	6,8,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	3,5,10,12,14,16	6,8	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	3,5,10,12,14,17	6,8,15,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	3,5,10,12,14,16,18	6,8,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	3,5,10,12,18	6,8,13,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,5,10,12,16,17	6,8,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	3,5,10,12	6,8,13,15	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,5,10,12,16,17,18	6,8,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	3,5,10,12,14,17	6,8,13,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,10,12,14,16,18	6,8,13,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	3,5,10,12,14,17,18	6,8,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,10,12,14,16	6,8,13,15	2^{-23}

Table 0.364 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	3,5,10,17	6,8,11,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	3,5,10,16,18	6,8,11,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	3,5,10,17,18	6,8,11,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	3,5,10,16	6,8,11,15	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	3,5,10,14,18	6,8,11,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	3,5,10,14,16,17	6,8,11,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	3,5,10,14	6,8,11,15	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	3,5,10,14,16,17,18	6,8,11,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	3,5,10,17,18	6,8,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	3,5,10,16	6,8,11,13	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	3,5,10,17	6,8,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	3,5,10,16,18	6,8,11,13,15,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	3,5,10,14	6,8,11,13	2^{-34}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	3,5,10,14,16,17,18	6,8,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	3,5,10,14,18	6,8,11,13,15,18	2^{-34}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	3,5,10,14,16,17	6,8,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	3,5,10,12,18	6,8,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	3,5,10,12,16,17	6,8,11,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	3,5,10,12	6,8,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	3,5,10,12,16,17,18	6,8,11,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,10,12,14,17	6,8,11,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	3,5,10,12,14,16,18	6,8,11,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	3,5,10,12,14,17,18	6,8,11,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	3,5,10,12,14,16	6,8,11,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	3,5,10,12	6,8,11,13	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	3,5,10,12,16,17,18	6,8,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	3,5,10,12,18	6,8,11,13,15,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	3,5,10,12,16,17	6,8,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	3,5,10,12,14,17,18	6,8,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	3,5,10,12,14,16	6,8,11,13	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	3,5,10,12,14,17	6,8,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	3,5,10,12,14,16,18	6,8,11,13,15,18	2^{-12}

Table 0.365 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	3,5,18	6,8,9,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	3,5,16,17	6,8,9,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	3,5	6,8,9,15	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	3,5,16,17,18	6,8,9,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	3,5,14,17	6,8,9,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	3,5,14,16,18	6,8,9,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	3,5,14,17,18	6,8,9,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	3,5,14,16	6,8,9,15	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	3,5	6,8,9,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	3,5,16,17,18	6,8,9,13,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	3,5,18	6,8,9,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	3,5,16,17	6,8,9,13,15,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	3,5,14,17,18	6,8,9,13,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	3,5,14,16	6,8,9,13	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	3,5,14,17	6,8,9,13,15,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	3,5,14,16,18	6,8,9,13,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	3,5,12,17	6,8,9,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	3,5,12,16,18	6,8,9,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	3,5,12,17,18	6,8,9,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	3,5,12,16	6,8,9,15	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	3,5,12,14,18	6,8,9,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	3,5,12,14,16,17	6,8,9,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	3,5,12,14	6,8,9,15	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	3,5,12,14,16,17,18	6,8,9,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	3,5,12,17,18	6,8,9,13,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	3,5,12,16	6,8,9,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	3,5,12,17	6,8,9,13,15,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	3,5,12,16,18	6,8,9,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	3,5,12,14	6,8,9,13	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	3,5,12,14,16,17,18	6,8,9,13,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	3,5,12,14,18	6,8,9,13,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	3,5,12,14,16,17	6,8,9,13,15,17	2^{-23}

Table 0.366 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	3,5	6,8,9,11	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	3,5,16,17,18	6,8,9,11,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	3,5,18	6,8,9,11,15,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	3,5,16,17	6,8,9,11,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,14,17,18	6,8,9,11,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	3,5,14,16	6,8,9,11	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,14,17	6,8,9,11,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	3,5,14,16,18	6,8,9,11,15,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	3,5,18	6,8,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	3,5,16,17	6,8,9,11,13,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	3,5	6,8,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	3,5,16,17,18	6,8,9,11,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	3,5,14,17	6,8,9,11,13,17	2^{-34}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	3,5,14,16,18	6,8,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	3,5,14,17,18	6,8,9,11,13,15,17,18	2^{-34}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	3,5,14,16	6,8,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	3,5,12,17,18	6,8,9,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	3,5,12,16	6,8,9,11	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	3,5,12,17	6,8,9,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	3,5,12,16,18	6,8,9,11,15,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	3,5,12,14	6,8,9,11	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	3,5,12,14,16,17,18	6,8,9,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	3,5,12,14,18	6,8,9,11,15,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	3,5,12,14,16,17	6,8,9,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	3,5,12,17	6,8,9,11,13,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	3,5,12,16,18	6,8,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	3,5,12,17,18	6,8,9,11,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	3,5,12,16	6,8,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	3,5,12,14,18	6,8,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	3,5,12,14,16,17	6,8,9,11,13,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	3,5,12,14	6,8,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	3,5,12,14,16,17,18	6,8,9,11,13,15,17,18	2^{-12}

Table 0.367 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	3,5,10,17	6,8,9,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	3,5,10,16,18	6,8,9,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	3,5,10,17,18	6,8,9,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	3,5,10,16	6,8,9,15	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	3,5,10,14,18	6,8,9,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	3,5,10,14,16,17	6,8,9,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	3,5,10,14	6,8,9,15	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	3,5,10,14,16,17,18	6,8,9,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	3,5,10,17,18	6,8,9,13,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,10,16	6,8,9,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	3,5,10,17	6,8,9,13,15,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	3,5,10,16,18	6,8,9,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	3,5,10,14	6,8,9,13	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	3,5,10,14,16,17,18	6,8,9,13,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	3,5,10,14,18	6,8,9,13,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	3,5,10,14,16,17	6,8,9,13,15,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	3,5,10,12,18	6,8,9,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	3,5,10,12,16,17	6,8,9,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	3,5,10,12	6,8,9,15	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	3,5,10,12,16,17,18	6,8,9,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	3,5,10,12,14,17	6,8,9,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	3,5,10,12,14,16,18	6,8,9,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	3,5,10,12,14,17,18	6,8,9,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	3,5,10,12,14,16	6,8,9,15	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	3,5,10,12	6,8,9,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	3,5,10,12,16,17,18	6,8,9,13,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	3,5,10,12,18	6,8,9,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	3,5,10,12,16,17	6,8,9,13,15,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	3,5,10,12,14,17,18	6,8,9,13,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	3,5,10,12,14,16	6,8,9,13	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	3,5,10,12,14,17	6,8,9,13,15,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	3,5,10,12,14,16,18	6,8,9,13,15,18	$2^{-6.5}$

Table 0.368 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	3,5,10,17,18	6,8,9,11,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	3,5,10,16	6,8,9,11	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	3,5,10,17	6,8,9,11,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	3,5,10,16,18	6,8,9,11,15,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	3,5,10,14	6,8,9,11	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	3,5,10,14,16,17,18	6,8,9,11,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	3,5,10,14,18	6,8,9,11,15,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	3,5,10,14,16,17	6,8,9,11,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	3,5,10,17	6,8,9,11,13,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	3,5,10,16,18	6,8,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	3,5,10,17,18	6,8,9,11,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	3,5,10,16	6,8,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	3,5,10,14,18	6,8,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	3,5,10,14,16,17	6,8,9,11,13,17	2^{-1}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	3,5,10,14	6,8,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	3,5,10,14,16,17,18	6,8,9,11,13,15,17,18	2^{-1}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5,10,12	6,8,9,11	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	3,5,10,12,16,17,18	6,8,9,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5,10,12,18	6,8,9,11,15,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	3,5,10,12,16,17	6,8,9,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	3,5,10,12,14,17,18	6,8,9,11,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,10,12,14,16	6,8,9,11	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	3,5,10,12,14,17	6,8,9,11,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,10,12,14,16,18	6,8,9,11,15,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	3,5,10,12,18	6,8,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	3,5,10,12,16,17	6,8,9,11,13,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	3,5,10,12	6,8,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	3,5,10,12,16,17,18	6,8,9,11,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,5,10,12,14,17	6,8,9,11,13,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,5,10,12,14,16,18	6,8,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	3,5,10,12,14,17,18	6,8,9,11,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	3,5,10,12,14,16	6,8,9,11,13,15	$2^{-17.5}$

Table 0.369 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	3,5,7,17	6,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	3,5,7,16,18	6,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	3,5,7,17,18	6,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	3,5,7,16	6,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	3,5,7,14,18	6,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	3,5,7,14,16,17	6,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	3,5,7,14	6,15	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	3,5,7,14,16,17,18	6,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	3,5,7,17,18	6,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	3,5,7,16	6,13	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	3,5,7,17	6,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	3,5,7,16,18	6,13,15,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	3,5,7,14	6,13	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	3,5,7,14,16,17,18	6,13,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	3,5,7,14,18	6,13,15,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	3,5,7,14,16,17	6,13,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	3,5,7,12,18	6,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	3,5,7,12,16,17	6,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	3,5,7,12	6,15	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	3,5,7,12,16,17,18	6,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	3,5,7,12,14,17	6,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	3,5,7,12,14,16,18	6,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	3,5,7,12,14,17,18	6,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	3,5,7,12,14,16	6,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	3,5,7,12	6,13	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	3,5,7,12,16,17,18	6,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	3,5,7,12,18	6,13,15,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	3,5,7,12,16,17	6,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	3,5,7,12,14,17,18	6,13,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	3,5,7,12,14,16	6,13	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	3,5,7,12,14,17	6,13,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	3,5,7,12,14,16,18	6,13,15,18	2^{-12}

Table 0.370 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	3,5,7,17,18	6,11,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	3,5,7,16	6,11	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	3,5,7,17	6,11,15,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	3,5,7,16,18	6,11,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	3,5,7,14	6,11	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	3,5,7,14,16,17,18	6,11,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	3,5,7,14,18	6,11,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	3,5,7,14,16,17	6,11,15,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	3,5,7,17	6,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	3,5,7,16,18	6,11,13,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	3,5,7,17,18	6,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	3,5,7,16	6,11,13,15	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	3,5,7,14,18	6,11,13,18	2^{-1}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	3,5,7,14,16,17	6,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	3,5,7,14	6,11,13,15	2^{-1}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	3,5,7,14,16,17,18	6,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	3,5,7,12	6,11	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	3,5,7,12,16,17,18	6,11,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	3,5,7,12,18	6,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	3,5,7,12,16,17	6,11,15,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	3,5,7,12,14,17,18	6,11,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	3,5,7,12,14,16	6,11	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	3,5,7,12,14,17	6,11,15,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	3,5,7,12,14,16,18	6,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	3,5,7,12,18	6,11,13,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	3,5,7,12,16,17	6,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	3,5,7,12	6,11,13,15	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	3,5,7,12,16,17,18	6,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,7,12,14,17	6,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	3,5,7,12,14,16,18	6,11,13,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,7,12,14,17,18	6,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	3,5,7,12,14,16	6,11,13,15	2^{-23}

Table 0.371 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	3,5,7,10,18	6,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	3,5,7,10,16,17	6,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,7,10	6,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	3,5,7,10,16,17,18	6,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	3,5,7,10,14,17	6,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	3,5,7,10,14,16,18	6,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	3,5,7,10,14,17,18	6,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	3,5,7,10,14,16	6,15	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	3,5,7,10	6,13	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	3,5,7,10,16,17,18	6,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	3,5,7,10,18	6,13,15,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	3,5,7,10,16,17	6,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	3,5,7,10,14,17,18	6,13,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	3,5,7,10,14,16	6,13	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	3,5,7,10,14,17	6,13,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	3,5,7,10,14,16,18	6,13,15,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	3,5,7,10,12,17	6,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	3,5,7,10,12,16,18	6,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	3,5,7,10,12,17,18	6,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	3,5,7,10,12,16	6,15	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	3,5,7,10,12,14,18	6,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	3,5,7,10,12,14,16,17	6,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	3,5,7,10,12,14	6,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	3,5,7,10,12,14,16,17,18	6,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	3,5,7,10,12,17,18	6,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	3,5,7,10,12,16	6,13	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	3,5,7,10,12,17	6,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	3,5,7,10,12,16,18	6,13,15,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	3,5,7,10,12,14	6,13	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	3,5,7,10,12,14,16,17,18	6,13,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	3,5,7,10,12,14,18	6,13,15,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	3,5,7,10,12,14,16,17	6,13,15,17	$2^{-28.5}$

Table 0.372 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	3,5,7,10	6,11	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	3,5,7,10,16,17,18	6,11,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	3,5,7,10,18	6,11,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	3,5,7,10,16,17	6,11,15,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	3,5,7,10,14,17,18	6,11,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	3,5,7,10,14,16	6,11	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	3,5,7,10,14,17	6,11,15,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	3,5,7,10,14,16,18	6,11,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	3,5,7,10,18	6,11,13,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	3,5,7,10,16,17	6,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	3,5,7,10	6,11,13,15	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	3,5,7,10,16,17,18	6,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	3,5,7,10,14,17	6,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	3,5,7,10,14,16,18	6,11,13,18	2^{-34}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	3,5,7,10,14,17,18	6,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	3,5,7,10,14,16	6,11,13,15	2^{-34}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	3,5,7,10,12,17,18	6,11,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	3,5,7,10,12,16	6,11	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	3,5,7,10,12,17	6,11,15,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	3,5,7,10,12,16,18	6,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	3,5,7,10,12,14	6,11	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	3,5,7,10,12,14,16,17,18	6,11,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	3,5,7,10,12,14,18	6,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	3,5,7,10,12,14,16,17	6,11,15,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	3,5,7,10,12,17	6,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	3,5,7,10,12,16,18	6,11,13,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	3,5,7,10,12,17,18	6,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,7,10,12,16	6,11,13,15	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	3,5,7,10,12,14,18	6,11,13,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,7,10,12,14,16,17	6,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	3,5,7,10,12,14	6,11,13,15	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,7,10,12,14,16,17,18	6,11,13,15,17,18	$2^{-17.5}$

Table 0.373 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	3,5,7,17,18	6,9,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	3,5,7,16	6,9	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	3,5,7,17	6,9,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	3,5,7,16,18	6,9,15,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	3,5,7,14	6,9	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	3,5,7,14,16,17,18	6,9,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	3,5,7,14,18	6,9,15,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	3,5,7,14,16,17	6,9,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	3,5,7,17	6,9,13,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	3,5,7,16,18	6,9,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	3,5,7,17,18	6,9,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	3,5,7,16	6,9,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	3,5,7,14,18	6,9,13,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	3,5,7,14,16,17	6,9,13,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	3,5,7,14	6,9,13,15	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	3,5,7,14,16,17,18	6,9,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	3,5,7,12	6,9	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5,7,12,16,17,18	6,9,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	3,5,7,12,18	6,9,15,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5,7,12,16,17	6,9,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,12,14,17,18	6,9,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	3,5,7,12,14,16	6,9	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,12,14,17	6,9,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	3,5,7,12,14,16,18	6,9,15,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	3,5,7,12,18	6,9,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	3,5,7,12,16,17	6,9,13,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	3,5,7,12	6,9,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	3,5,7,12,16,17,18	6,9,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	3,5,7,12,14,17	6,9,13,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	3,5,7,12,14,16,18	6,9,13,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,5,7,12,14,17,18	6,9,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,5,7,12,14,16	6,9,13,15	$2^{-28.5}$

Table 0.374 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	3,5,7,17	6,9,11,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	3,5,7,16,18	6,9,11,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	3,5,7,17,18	6,9,11,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	3,5,7,16	6,9,11,15	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	3,5,7,14,18	6,9,11,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	3,5,7,14,16,17	6,9,11,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	3,5,7,14	6,9,11,15	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	3,5,7,14,16,17,18	6,9,11,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,7,17,18	6,9,11,13,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	3,5,7,16	6,9,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,7,17	6,9,11,13,15,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	3,5,7,16,18	6,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	3,5,7,14	6,9,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	3,5,7,14,16,17,18	6,9,11,13,17,18	2^{-34}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	3,5,7,14,18	6,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	3,5,7,14,16,17	6,9,11,13,15,17	2^{-34}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	3,5,7,12,18	6,9,11,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	3,5,7,12,16,17	6,9,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	3,5,7,12	6,9,11,15	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	3,5,7,12,16,17,18	6,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	3,5,7,12,14,17	6,9,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	3,5,7,12,14,16,18	6,9,11,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	3,5,7,12,14,17,18	6,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	3,5,7,12,14,16	6,9,11,15	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	3,5,7,12	6,9,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	3,5,7,12,16,17,18	6,9,11,13,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	3,5,7,12,18	6,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	3,5,7,12,16,17	6,9,11,13,15,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	3,5,7,12,14,17,18	6,9,11,13,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	3,5,7,12,14,16	6,9,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	3,5,7,12,14,17	6,9,11,13,15,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	3,5,7,12,14,16,18	6,9,11,13,15,18	$2^{-17.5}$

Table 0.375 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,10	6,9	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	3,5,7,10,16,17,18	6,9,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,10,18	6,9,15,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	3,5,7,10,16,17	6,9,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	3,5,7,10,14,17,18	6,9,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,10,14,16	6,9	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	3,5,7,10,14,17	6,9,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,10,14,16,18	6,9,15,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	3,5,7,10,18	6,9,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	3,5,7,10,16,17	6,9,13,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	3,5,7,10	6,9,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	3,5,7,10,16,17,18	6,9,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	3,5,7,10,14,17	6,9,13,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	3,5,7,10,14,16,18	6,9,13,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	3,5,7,10,14,17,18	6,9,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	3,5,7,10,14,16	6,9,13,15	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	3,5,7,10,12,17,18	6,9,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	3,5,7,10,12,16	6,9	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	3,5,7,10,12,17	6,9,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	3,5,7,10,12,16,18	6,9,15,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	3,5,7,10,12,14	6,9	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	3,5,7,10,12,14,16,17,18	6,9,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	3,5,7,10,12,14,18	6,9,15,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	3,5,7,10,12,14,16,17	6,9,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	3,5,7,10,12,17	6,9,13,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	3,5,7,10,12,16,18	6,9,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	3,5,7,10,12,17,18	6,9,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	3,5,7,10,12,16	6,9,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	3,5,7,10,12,14,18	6,9,13,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	3,5,7,10,12,14,16,17	6,9,13,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	3,5,7,10,12,14	6,9,13,15	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	3,5,7,10,12,14,16,17,18	6,9,13,15,17,18	2^{-12}

Table 0.376 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	3,5,7,10,18	6,9,11,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	3,5,7,10,16,17	6,9,11,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	3,5,7,10	6,9,11,15	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	3,5,7,10,16,17,18	6,9,11,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	3,5,7,10,14,17	6,9,11,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	3,5,7,10,14,16,18	6,9,11,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	3,5,7,10,14,17,18	6,9,11,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	3,5,7,10,14,16	6,9,11,15	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	3,5,7,10	6,9,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	3,5,7,10,16,17,18	6,9,11,13,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	3,5,7,10,18	6,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	3,5,7,10,16,17	6,9,11,13,15,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	3,5,7,10,14,17,18	6,9,11,13,17,18	2^{-1}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	3,5,7,10,14,16	6,9,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	3,5,7,10,14,17	6,9,11,13,15,17	2^{-1}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	3,5,7,10,14,16,18	6,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	3,5,7,10,12,17	6,9,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	3,5,7,10,12,16,18	6,9,11,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	3,5,7,10,12,17,18	6,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	3,5,7,10,12,16	6,9,11,15	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	3,5,7,10,12,14,18	6,9,11,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	3,5,7,10,12,14,16,17	6,9,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	3,5,7,10,12,14	6,9,11,15	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	3,5,7,10,12,14,16,17,18	6,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	3,5,7,10,12,17,18	6,9,11,13,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	3,5,7,10,12,16	6,9,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	3,5,7,10,12,17	6,9,11,13,15,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	3,5,7,10,12,16,18	6,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	3,5,7,10,12,14	6,9,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	3,5,7,10,12,14,16,17,18	6,9,11,13,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	3,5,7,10,12,14,18	6,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	3,5,7,10,12,14,16,17	6,9,11,13,15,17	2^{-23}

Table 0.377 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	3,5,7,18	6,8,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,16,17	6,8,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	3,5,7	6,8,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,16,17,18	6,8,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,14,17	6,8,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	3,5,7,14,16,18	6,8,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,14,17,18	6,8,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	3,5,7,14,16	6,8,15	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	3,5,7	6,8,13	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	3,5,7,16,17,18	6,8,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	3,5,7,18	6,8,13,15,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	3,5,7,16,17	6,8,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	3,5,7,14,17,18	6,8,13,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	3,5,7,14,16	6,8,13	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	3,5,7,14,17	6,8,13,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	3,5,7,14,16,18	6,8,13,15,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	3,5,7,12,17	6,8,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	3,5,7,12,16,18	6,8,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	3,5,7,12,17,18	6,8,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	3,5,7,12,16	6,8,15	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	3,5,7,12,14,18	6,8,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	3,5,7,12,14,16,17	6,8,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	3,5,7,12,14	6,8,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	3,5,7,12,14,16,17,18	6,8,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	3,5,7,12,17,18	6,8,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	3,5,7,12,16	6,8,13	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	3,5,7,12,17	6,8,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	3,5,7,12,16,18	6,8,13,15,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	3,5,7,12,14	6,8,13	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	3,5,7,12,14,16,17,18	6,8,13,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	3,5,7,12,14,18	6,8,13,15,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	3,5,7,12,14,16,17	6,8,13,15,17	$2^{-6.5}$

Table 0.378 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	3,5,7	6,8,11	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	3,5,7,16,17,18	6,8,11,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	3,5,7,18	6,8,11,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	3,5,7,16,17	6,8,11,15,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	3,5,7,14,17,18	6,8,11,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	3,5,7,14,16	6,8,11	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	3,5,7,14,17	6,8,11,15,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	3,5,7,14,16,18	6,8,11,15,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	3,5,7,18	6,8,11,13,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	3,5,7,16,17	6,8,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	3,5,7	6,8,11,13,15	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	3,5,7,16,17,18	6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	3,5,7,14,17	6,8,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	3,5,7,14,16,18	6,8,11,13,18	2^{-1}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	3,5,7,14,17,18	6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	3,5,7,14,16	6,8,11,13,15	2^{-1}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	3,5,7,12,17,18	6,8,11,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	3,5,7,12,16	6,8,11	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	3,5,7,12,17	6,8,11,15,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	3,5,7,12,16,18	6,8,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	3,5,7,12,14	6,8,11	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	3,5,7,12,14,16,17,18	6,8,11,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	3,5,7,12,14,18	6,8,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	3,5,7,12,14,16,17	6,8,11,15,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	3,5,7,12,17	6,8,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	3,5,7,12,16,18	6,8,11,13,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	3,5,7,12,17,18	6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	3,5,7,12,16	6,8,11,13,15	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	3,5,7,12,14,18	6,8,11,13,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	3,5,7,12,14,16,17	6,8,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	3,5,7,12,14	6,8,11,13,15	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	3,5,7,12,14,16,17,18	6,8,11,13,15,17,18	$2^{-17.5}$

Table 0.379 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	3,5,7,10,17	6,8,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	3,5,7,10,16,18	6,8,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	3,5,7,10,17,18	6,8,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	3,5,7,10,16	6,8,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	3,5,7,10,14,18	6,8,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	3,5,7,10,14,16,17	6,8,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	3,5,7,10,14	6,8,15	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	3,5,7,10,14,16,17,18	6,8,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	3,5,7,10,17,18	6,8,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	3,5,7,10,16	6,8,13	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	3,5,7,10,17	6,8,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	3,5,7,10,16,18	6,8,13,15,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	3,5,7,10,14	6,8,13	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	3,5,7,10,14,16,17,18	6,8,13,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	3,5,7,10,14,18	6,8,13,15,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	3,5,7,10,14,16,17	6,8,13,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5,7,10,12,18	6,8,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	3,5,7,10,12,16,17	6,8,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5,7,10,12	6,8,15	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	3,5,7,10,12,16,17,18	6,8,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	3,5,7,10,12,14,17	6,8,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,10,12,14,16,18	6,8,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	3,5,7,10,12,14,17,18	6,8,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,10,12,14,16	6,8,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	3,5,7,10,12	6,8,13	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	3,5,7,10,12,16,17,18	6,8,13,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	3,5,7,10,12,18	6,8,13,15,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	3,5,7,10,12,16,17	6,8,13,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	3,5,7,10,12,14,17,18	6,8,13,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	3,5,7,10,12,14,16	6,8,13	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,5,7,10,12,14,17	6,8,13,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,5,7,10,12,14,16,18	6,8,13,15,18	2^{-23}

Table 0.380 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	3,5,7,10,17,18	6,8,11,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	3,5,7,10,16	6,8,11	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	3,5,7,10,17	6,8,11,15,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	3,5,7,10,16,18	6,8,11,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	3,5,7,10,14	6,8,11	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	3,5,7,10,14,16,17,18	6,8,11,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	3,5,7,10,14,18	6,8,11,15,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	3,5,7,10,14,16,17	6,8,11,15,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	3,5,7,10,17	6,8,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	3,5,7,10,16,18	6,8,11,13,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	3,5,7,10,17,18	6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,7,10,16	6,8,11,13,15	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	3,5,7,10,14,18	6,8,11,13,18	2^{-34}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	3,5,7,10,14,16,17	6,8,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	3,5,7,10,14	6,8,11,13,15	2^{-34}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	3,5,7,10,14,16,17,18	6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	3,5,7,10,12	6,8,11	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	3,5,7,10,12,16,17,18	6,8,11,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	3,5,7,10,12,18	6,8,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	3,5,7,10,12,16,17	6,8,11,15,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	3,5,7,10,12,14,17,18	6,8,11,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	3,5,7,10,12,14,16	6,8,11	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	3,5,7,10,12,14,17	6,8,11,15,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	3,5,7,10,12,14,16,18	6,8,11,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	3,5,7,10,12,18	6,8,11,13,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	3,5,7,10,12,16,17	6,8,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	3,5,7,10,12	6,8,11,13,15	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	3,5,7,10,12,16,17,18	6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	3,5,7,10,12,14,17	6,8,11,13,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	3,5,7,10,12,14,16,18	6,8,11,13,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	3,5,7,10,12,14,17,18	6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	3,5,7,10,12,14,16	6,8,11,13,15	2^{-12}

Table 0.381 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	3,5,7	6,8,9	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	3,5,7,16,17,18	6,8,9,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	3,5,7,18	6,8,9,15,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	3,5,7,16,17	6,8,9,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	3,5,7,14,17,18	6,8,9,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	3,5,7,14,16	6,8,9	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	3,5,7,14,17	6,8,9,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	3,5,7,14,16,18	6,8,9,15,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	3,5,7,18	6,8,9,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	3,5,7,16,17	6,8,9,13,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	3,5,7	6,8,9,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	3,5,7,16,17,18	6,8,9,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	3,5,7,14,17	6,8,9,13,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	3,5,7,14,16,18	6,8,9,13,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	3,5,7,14,17,18	6,8,9,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	3,5,7,14,16	6,8,9,13,15	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	3,5,7,12,17,18	6,8,9,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	3,5,7,12,16	6,8,9	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	3,5,7,12,17	6,8,9,15,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	3,5,7,12,16,18	6,8,9,15,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	3,5,7,12,14	6,8,9	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	3,5,7,12,14,16,17,18	6,8,9,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	3,5,7,12,14,18	6,8,9,15,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	3,5,7,12,14,16,17	6,8,9,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	3,5,7,12,17	6,8,9,13,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	3,5,7,12,16,18	6,8,9,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	3,5,7,12,17,18	6,8,9,13,15,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	3,5,7,12,16	6,8,9,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	3,5,7,12,14,18	6,8,9,13,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	3,5,7,12,14,16,17	6,8,9,13,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	3,5,7,12,14	6,8,9,13,15	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	3,5,7,12,14,16,17,18	6,8,9,13,15,17,18	2^{-23}

Table 0.382 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	3,5,7,18	6,8,9,11,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	3,5,7,16,17	6,8,9,11,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	3,5,7	6,8,9,11,15	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	3,5,7,16,17,18	6,8,9,11,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	3,5,7,14,17	6,8,9,11,17	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	3,5,7,14,16,18	6,8,9,11,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	3,5,7,14,17,18	6,8,9,11,15,17,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	3,5,7,14,16	6,8,9,11,15	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	3,5,7	6,8,9,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	3,5,7,16,17,18	6,8,9,11,13,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	3,5,7,18	6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	3,5,7,16,17	6,8,9,11,13,15,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	3,5,7,14,17,18	6,8,9,11,13,17,18	2^{-34}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	3,5,7,14,16	6,8,9,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	3,5,7,14,17	6,8,9,11,13,15,17	2^{-34}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	3,5,7,14,16,18	6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	3,5,7,12,17	6,8,9,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	3,5,7,12,16,18	6,8,9,11,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	3,5,7,12,17,18	6,8,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	3,5,7,12,16	6,8,9,11,15	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	3,5,7,12,14,18	6,8,9,11,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	3,5,7,12,14,16,17	6,8,9,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	3,5,7,12,14	6,8,9,11,15	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	3,5,7,12,14,16,17,18	6,8,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	3,5,7,12,17,18	6,8,9,11,13,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	3,5,7,12,16	6,8,9,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,7,12,17	6,8,9,11,13,15,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	3,5,7,12,16,18	6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,7,12,14	6,8,9,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	3,5,7,12,14,16,17,18	6,8,9,11,13,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,7,12,14,18	6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	3,5,7,12,14,16,17	6,8,9,11,13,15,17	2^{-12}

Table 0.383 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	3,5,7,10,17,18	6,8,9,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	3,5,7,10,16	6,8,9	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	3,5,7,10,17	6,8,9,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	3,5,7,10,16,18	6,8,9,15,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	3,5,7,10,14	6,8,9	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	3,5,7,10,14,16,17,18	6,8,9,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	3,5,7,10,14,18	6,8,9,15,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	3,5,7,10,14,16,17	6,8,9,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	3,5,7,10,17	6,8,9,13,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	3,5,7,10,16,18	6,8,9,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	3,5,7,10,17,18	6,8,9,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	3,5,7,10,16	6,8,9,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	3,5,7,10,14,18	6,8,9,13,18	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	3,5,7,10,14,16,17	6,8,9,13,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	3,5,7,10,14	6,8,9,13,15	$2^{-28.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	3,5,7,10,14,16,17,18	6,8,9,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	3,5,7,10,12	6,8,9	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	3,5,7,10,12,16,17,18	6,8,9,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	3,5,7,10,12,18	6,8,9,15,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	3,5,7,10,12,16,17	6,8,9,15,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	3,5,7,10,12,14,17,18	6,8,9,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	3,5,7,10,12,14,16	6,8,9	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	3,5,7,10,12,14,17	6,8,9,15,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	3,5,7,10,12,14,16,18	6,8,9,15,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	3,5,7,10,12,18	6,8,9,13,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	3,5,7,10,12,16,17	6,8,9,13,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	3,5,7,10,12	6,8,9,13,15	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	3,5,7,10,12,16,17,18	6,8,9,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	3,5,7,10,12,14,17	6,8,9,13,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	3,5,7,10,12,14,16,18	6,8,9,13,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	3,5,7,10,12,14,17,18	6,8,9,13,15,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	3,5,7,10,12,14,16	6,8,9,13,15	$2^{-6.5}$

Table 0.384 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	3,5,7,10,17	6,8,9,11,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	3,5,7,10,16,18	6,8,9,11,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	3,5,7,10,17,18	6,8,9,11,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	3,5,7,10,16	6,8,9,11,15	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	3,5,7,10,14,18	6,8,9,11,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	3,5,7,10,14,16,17	6,8,9,11,17	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	3,5,7,10,14	6,8,9,11,15	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	3,5,7,10,14,16,17,18	6,8,9,11,15,17,18	$2^{-6.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	3,5,7,10,17,18	6,8,9,11,13,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	3,5,7,10,16	6,8,9,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	3,5,7,10,17	6,8,9,11,13,15,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	3,5,7,10,16,18	6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	3,5,7,10,14	6,8,9,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	3,5,7,10,14,16,17,18	6,8,9,11,13,17,18	2^{-1}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	3,5,7,10,14,18	6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	3,5,7,10,14,16,17	6,8,9,11,13,15,17	2^{-1}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	3,5,7,10,12,18	6,8,9,11,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	3,5,7,10,12,16,17	6,8,9,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	3,5,7,10,12	6,8,9,11,15	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	3,5,7,10,12,16,17,18	6,8,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	3,5,7,10,12,14,17	6,8,9,11,17	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	3,5,7,10,12,14,16,18	6,8,9,11,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	3,5,7,10,12,14,17,18	6,8,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	3,5,7,10,12,14,16	6,8,9,11,15	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	3,5,7,10,12	6,8,9,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	3,5,7,10,12,16,17,18	6,8,9,11,13,17,18	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	3,5,7,10,12,18	6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	3,5,7,10,12,16,17	6,8,9,11,13,15,17	2^{-12}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	3,5,7,10,12,14,17,18	6,8,9,11,13,17,18	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,7,10,12,14,16	6,8,9,11,13	$2^{-17.5}$
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	3,5,7,10,12,14,17	6,8,9,11,13,15,17	2^{-23}
$(0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,7,10,12,14,16,18	6,8,9,11,13,15,18	$2^{-17.5}$

Table 0.385 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	3,17	4,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	3,16,18	4,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	3,17,18	4,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	3,16	4,15	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	3,14,18	4,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	3,14,16,17	4,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	3,14	4,15	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	3,14,16,17,18	4,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	3,17,18	4,13,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	3,16	4,13	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	3,17	4,13,15,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	3,16,18	4,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	3,14	4,13	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	3,14,16,17,18	4,13,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	3,14,18	4,13,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	3,14,16,17	4,13,15,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	3,12,18	4,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	3,12,16,17	4,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	3,12	4,15	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	3,12,16,17,18	4,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	3,12,14,17	4,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,12,14,16,18	4,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	3,12,14,17,18	4,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	3,12,14,16	4,15	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	3,12	4,13	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	3,12,16,17,18	4,13,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	3,12,18	4,13,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	3,12,16,17	4,13,15,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	3,12,14,17,18	4,13,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	3,12,14,16	4,13	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	3,12,14,17	4,13,15,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	3,12,14,16,18	4,13,15,18	$2^{-17.5}$

Table 0.386 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	3,17,18	4,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	3,16	4,11	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	3,17	4,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	3,16,18	4,11,15,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	3,14	4,11	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	3,14,16,17,18	4,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	3,14,18	4,11,15,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	3,14,16,17	4,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	3,17	4,11,13,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	3,16,18	4,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	3,17,18	4,11,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	3,16	4,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	3,14,18	4,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	3,14,16,17	4,11,13,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	3,14	4,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	3,14,16,17,18	4,11,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	3,12	4,11	2^{-1}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	3,12,16,17,18	4,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	3,12,18	4,11,15,18	2^{-1}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	3,12,16,17	4,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	3,12,14,17,18	4,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	3,12,14,16	4,11	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	3,12,14,17	4,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	3,12,14,16,18	4,11,15,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	3,12,18	4,11,13,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	3,12,16,17	4,11,13,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	3,12	4,11,13,15	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	3,12,16,17,18	4,11,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	3,12,14,17	4,11,13,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	3,12,14,16,18	4,11,13,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	3,12,14,17,18	4,11,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	3,12,14,16	4,11,13,15	$2^{-6.5}$

Table 0.387 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	3,10,18	4,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	3,10,16,17	4,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	3,10	4,15	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	3,10,16,17,18	4,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,10,14,17	4,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	3,10,14,16,18	4,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	3,10,14,17,18	4,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	3,10,14,16	4,15	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	3,10	4,13	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	3,10,16,17,18	4,13,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	3,10,18	4,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	3,10,16,17	4,13,15,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,10,14,17,18	4,13,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,10,14,16	4,13	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	3,10,14,17	4,13,15,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	3,10,14,16,18	4,13,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	3,10,12,17	4,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	3,10,12,16,18	4,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	3,10,12,17,18	4,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	3,10,12,16	4,15	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	3,10,12,14,18	4,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	3,10,12,14,16,17	4,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	3,10,12,14	4,15	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	3,10,12,14,16,17,18	4,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	3,10,12,17,18	4,13,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	3,10,12,16	4,13	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	3,10,12,17	4,13,15,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	3,10,12,16,18	4,13,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	3,10,12,14	4,13	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	3,10,12,14,16,17,18	4,13,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	3,10,12,14,18	4,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	3,10,12,14,16,17	4,13,15,17	2^{-12}

Table 0.388 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	3,10	4,11	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	3,10,16,17,18	4,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	3,10,18	4,11,15,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	3,10,16,17	4,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	3,10,14,17,18	4,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	3,10,14,16	4,11	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	3,10,14,17	4,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	3,10,14,16,18	4,11,15,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	3,10,18	4,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	3,10,16,17	4,11,13,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	3,10	4,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	3,10,16,17,18	4,11,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	3,10,14,17	4,11,13,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	3,10,14,16,18	4,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	3,10,14,17,18	4,11,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	3,10,14,16	4,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	3,10,12,17,18	4,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	3,10,12,16	4,11	2^{-34}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	3,10,12,17	4,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	3,10,12,16,18	4,11,15,18	2^{-34}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	3,10,12,14	4,11	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	3,10,12,14,16,17,18	4,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	3,10,12,14,18	4,11,15,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	3,10,12,14,16,17	4,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	3,10,12,17	4,11,13,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	3,10,12,16,18	4,11,13,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	3,10,12,17,18	4,11,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	3,10,12,16	4,11,13,15	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	3,10,12,14,18	4,11,13,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	3,10,12,14,16,17	4,11,13,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	3,10,12,14	4,11,13,15	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	3,10,12,14,16,17,18	4,11,13,15,17,18	2^{-23}

Table 0.389 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	3,17,18	4,9,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	3,16	4,9	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	3,17	4,9,15,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	3,16,18	4,9,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	3,14	4,9	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	3,14,16,17,18	4,9,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	3,14,18	4,9,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	3,14,16,17	4,9,15,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	3,17	4,9,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	3,16,18	4,9,13,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	3,17,18	4,9,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	3,16	4,9,13,15	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	3,14,18	4,9,13,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	3,14,16,17	4,9,13,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	3,14	4,9,13,15	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	3,14,16,17,18	4,9,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	3,12	4,9	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	3,12,16,17,18	4,9,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	3,12,18	4,9,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	3,12,16,17	4,9,15,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	3,12,14,17,18	4,9,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	3,12,14,16	4,9	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	3,12,14,17	4,9,15,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	3,12,14,16,18	4,9,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	3,12,18	4,9,13,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	3,12,16,17	4,9,13,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	3,12	4,9,13,15	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	3,12,16,17,18	4,9,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	3,12,14,17	4,9,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	3,12,14,16,18	4,9,13,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	3,12,14,17,18	4,9,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	3,12,14,16	4,9,13,15	2^{-12}

Table 0.390 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	3,17	4,9,11,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	3,16,18	4,9,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	3,17,18	4,9,11,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	3,16	4,9,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	3,14,18	4,9,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	3,14,16,17	4,9,11,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	3,14	4,9,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	3,14,16,17,18	4,9,11,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	3,17,18	4,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	3,16	4,9,11,13	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	3,17	4,9,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	3,16,18	4,9,11,13,15,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	3,14	4,9,11,13	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,14,16,17,18	4,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	3,14,18	4,9,11,13,15,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	3,14,16,17	4,9,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	3,12,18	4,9,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	3,12,16,17	4,9,11,17	2^{-34}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	3,12	4,9,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	3,12,16,17,18	4,9,11,15,17,18	2^{-34}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	3,12,14,17	4,9,11,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	3,12,14,16,18	4,9,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	3,12,14,17,18	4,9,11,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	3,12,14,16	4,9,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	3,12	4,9,11,13	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	3,12,16,17,18	4,9,11,13,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	3,12,18	4,9,11,13,15,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	3,12,16,17	4,9,11,13,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	3,12,14,17,18	4,9,11,13,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	3,12,14,16	4,9,11,13	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	3,12,14,17	4,9,11,13,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	3,12,14,16,18	4,9,11,13,15,18	2^{-23}

Table 0.391 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	3,10	4,9	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	3,10,16,17,18	4,9,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	3,10,18	4,9,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	3,10,16,17	4,9,15,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	3,10,14,17,18	4,9,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	3,10,14,16	4,9	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	3,10,14,17	4,9,15,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	3,10,14,16,18	4,9,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	3,10,18	4,9,13,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	3,10,16,17	4,9,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	3,10	4,9,13,15	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	3,10,16,17,18	4,9,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	3,10,14,17	4,9,13,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	3,10,14,16,18	4,9,13,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	3,10,14,17,18	4,9,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	3,10,14,16	4,9,13,15	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	3,10,12,17,18	4,9,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	3,10,12,16	4,9	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	3,10,12,17	4,9,15,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	3,10,12,16,18	4,9,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	3,10,12,14	4,9	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	3,10,12,14,16,17,18	4,9,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	3,10,12,14,18	4,9,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	3,10,12,14,16,17	4,9,15,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	3,10,12,17	4,9,13,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	3,10,12,16,18	4,9,13,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	3,10,12,17,18	4,9,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	3,10,12,16	4,9,13,15	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	3,10,12,14,18	4,9,13,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	3,10,12,14,16,17	4,9,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	3,10,12,14	4,9,13,15	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	3,10,12,14,16,17,18	4,9,13,15,17,18	$2^{-17.5}$

Table 0.392 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	3,10,18	4,9,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	3,10,16,17	4,9,11,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	3,10	4,9,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	3,10,16,17,18	4,9,11,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	3,10,14,17	4,9,11,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	3,10,14,16,18	4,9,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	3,10,14,17,18	4,9,11,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	3,10,14,16	4,9,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	3,10	4,9,11,13	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	3,10,16,17,18	4,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	3,10,18	4,9,11,13,15,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	3,10,16,17	4,9,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,10,14,17,18	4,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	3,10,14,16	4,9,11,13	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	3,10,14,17	4,9,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	3,10,14,16,18	4,9,11,13,15,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	3,10,12,17	4,9,11,17	2^{-1}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	3,10,12,16,18	4,9,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	3,10,12,17,18	4,9,11,15,17,18	2^{-1}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	3,10,12,16	4,9,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	3,10,12,14,18	4,9,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	3,10,12,14,16,17	4,9,11,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	3,10,12,14	4,9,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	3,10,12,14,16,17,18	4,9,11,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	3,10,12,17,18	4,9,11,13,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	3,10,12,16	4,9,11,13	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	3,10,12,17	4,9,11,13,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	3,10,12,16,18	4,9,11,13,15,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	3,10,12,14	4,9,11,13	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	3,10,12,14,16,17,18	4,9,11,13,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	3,10,12,14,18	4,9,11,13,15,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	3,10,12,14,16,17	4,9,11,13,15,17	$2^{-6.5}$

Table 0.393 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	3,18	4,8,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	3,16,17	4,8,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	3	4,8,15	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	3,16,17,18	4,8,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	3,14,17	4,8,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	3,14,16,18	4,8,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	3,14,17,18	4,8,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	3,14,16	4,8,15	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	3	4,8,13	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	3,16,17,18	4,8,13,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	3,18	4,8,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	3,16,17	4,8,13,15,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	3,14,17,18	4,8,13,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	3,14,16	4,8,13	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	3,14,17	4,8,13,15,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	3,14,16,18	4,8,13,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	3,12,17	4,8,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	3,12,16,18	4,8,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	3,12,17,18	4,8,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	3,12,16	4,8,15	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	3,12,14,18	4,8,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	3,12,14,16,17	4,8,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	3,12,14	4,8,15	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	3,12,14,16,17,18	4,8,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	3,12,17,18	4,8,13,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	3,12,16	4,8,13	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	3,12,17	4,8,13,15,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	3,12,16,18	4,8,13,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	3,12,14	4,8,13	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	3,12,14,16,17,18	4,8,13,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	3,12,14,18	4,8,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	3,12,14,16,17	4,8,13,15,17	2^{-23}

Table 0.394 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	3	4,8,11	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	3,16,17,18	4,8,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	3,18	4,8,11,15,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	3,16,17	4,8,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	3,14,17,18	4,8,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	3,14,16	4,8,11	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	3,14,17	4,8,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	3,14,16,18	4,8,11,15,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	3,18	4,8,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	3,16,17	4,8,11,13,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	3	4,8,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	3,16,17,18	4,8,11,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	3,14,17	4,8,11,13,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,14,16,18	4,8,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	3,14,17,18	4,8,11,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	3,14,16	4,8,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	3,12,17,18	4,8,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	3,12,16	4,8,11	2^{-1}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	3,12,17	4,8,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	3,12,16,18	4,8,11,15,18	2^{-1}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	3,12,14	4,8,11	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	3,12,14,16,17,18	4,8,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	3,12,14,18	4,8,11,15,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	3,12,14,16,17	4,8,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	3,12,17	4,8,11,13,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	3,12,16,18	4,8,11,13,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	3,12,17,18	4,8,11,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	3,12,16	4,8,11,13,15	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	3,12,14,18	4,8,11,13,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	3,12,14,16,17	4,8,11,13,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	3,12,14	4,8,11,13,15	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	3,12,14,16,17,18	4,8,11,13,15,17,18	2^{-12}

Table 0.395 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	3,10,17	4,8,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	3,10,16,18	4,8,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	3,10,17,18	4,8,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	3,10,16	4,8,15	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	3,10,14,18	4,8,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	3,10,14,16,17	4,8,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	3,10,14	4,8,15	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	3,10,14,16,17,18	4,8,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	3,10,17,18	4,8,13,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	3,10,16	4,8,13	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	3,10,17	4,8,13,15,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	3,10,16,18	4,8,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	3,10,14	4,8,13	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	3,10,14,16,17,18	4,8,13,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	3,10,14,18	4,8,13,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	3,10,14,16,17	4,8,13,15,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	3,10,12,18	4,8,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	3,10,12,16,17	4,8,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	3,10,12	4,8,15	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	3,10,12,16,17,18	4,8,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	3,10,12,14,17	4,8,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	3,10,12,14,16,18	4,8,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	3,10,12,14,17,18	4,8,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	3,10,12,14,16	4,8,15	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	3,10,12	4,8,13	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	3,10,12,16,17,18	4,8,13,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	3,10,12,18	4,8,13,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	3,10,12,16,17	4,8,13,15,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	3,10,12,14,17,18	4,8,13,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	3,10,12,14,16	4,8,13	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	3,10,12,14,17	4,8,13,15,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	3,10,12,14,16,18	4,8,13,15,18	$2^{-17.5}$

Table 0.396 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	3,10,17,18	4,8,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	3,10,16	4,8,11	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	3,10,17	4,8,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	3,10,16,18	4,8,11,15,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	3,10,14	4,8,11	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	3,10,14,16,17,18	4,8,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	3,10,14,18	4,8,11,15,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	3,10,14,16,17	4,8,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	3,10,17	4,8,11,13,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	3,10,16,18	4,8,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	3,10,17,18	4,8,11,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	3,10,16	4,8,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,10,14,18	4,8,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	3,10,14,16,17	4,8,11,13,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	3,10,14	4,8,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	3,10,14,16,17,18	4,8,11,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	3,10,12	4,8,11	2^{-34}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	3,10,12,16,17,18	4,8,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	3,10,12,18	4,8,11,15,18	2^{-34}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	3,10,12,16,17	4,8,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	3,10,12,14,17,18	4,8,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	3,10,12,14,16	4,8,11	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	3,10,12,14,17	4,8,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	3,10,12,14,16,18	4,8,11,15,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	3,10,12,18	4,8,11,13,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	3,10,12,16,17	4,8,11,13,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	3,10,12	4,8,11,13,15	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	3,10,12,16,17,18	4,8,11,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	3,10,12,14,17	4,8,11,13,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	3,10,12,14,16,18	4,8,11,13,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	3,10,12,14,17,18	4,8,11,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	3,10,12,14,16	4,8,11,13,15	$2^{-28.5}$

Table 0.397 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	3	4,8,9	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	3,16,17,18	4,8,9,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	3,18	4,8,9,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	3,16,17	4,8,9,15,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	3,14,17,18	4,8,9,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,14,16	4,8,9	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	3,14,17	4,8,9,15,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	3,14,16,18	4,8,9,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	3,18	4,8,9,13,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	3,16,17	4,8,9,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	3	4,8,9,13,15	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	3,16,17,18	4,8,9,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,14,17	4,8,9,13,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,14,16,18	4,8,9,13,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	3,14,17,18	4,8,9,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	3,14,16	4,8,9,13,15	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	3,12,17,18	4,8,9,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	3,12,16	4,8,9	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	3,12,17	4,8,9,15,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	3,12,16,18	4,8,9,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	3,12,14	4,8,9	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	3,12,14,16,17,18	4,8,9,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	3,12,14,18	4,8,9,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	3,12,14,16,17	4,8,9,15,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	3,12,17	4,8,9,13,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	3,12,16,18	4,8,9,13,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	3,12,17,18	4,8,9,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	3,12,16	4,8,9,13,15	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	3,12,14,18	4,8,9,13,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	3,12,14,16,17	4,8,9,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	3,12,14	4,8,9,13,15	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	3,12,14,16,17,18	4,8,9,13,15,17,18	$2^{-17.5}$

Table 0.398 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	3,18	4,8,9,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	3,16,17	4,8,9,11,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	3	4,8,9,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	3,16,17,18	4,8,9,11,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	3,14,17	4,8,9,11,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	3,14,16,18	4,8,9,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	3,14,17,18	4,8,9,11,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	3,14,16	4,8,9,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	3	4,8,9,11,13	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	3,16,17,18	4,8,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	3,18	4,8,9,11,13,15,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	3,16,17	4,8,9,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	3,14,17,18	4,8,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	3,14,16	4,8,9,11,13	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	3,14,17	4,8,9,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	3,14,16,18	4,8,9,11,13,15,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	3,12,17	4,8,9,11,17	2^{-34}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	3,12,16,18	4,8,9,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	3,12,17,18	4,8,9,11,15,17,18	2^{-34}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	3,12,16	4,8,9,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	3,12,14,18	4,8,9,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	3,12,14,16,17	4,8,9,11,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	3,12,14	4,8,9,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	3,12,14,16,17,18	4,8,9,11,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	3,12,17,18	4,8,9,11,13,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	3,12,16	4,8,9,11,13	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	3,12,17	4,8,9,11,13,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	3,12,16,18	4,8,9,11,13,15,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	3,12,14	4,8,9,11,13	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	3,12,14,16,17,18	4,8,9,11,13,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	3,12,14,18	4,8,9,11,13,15,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	3,12,14,16,17	4,8,9,11,13,15,17	$2^{-28.5}$

Table 0.399 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	3,10,17,18	4,8,9,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	3,10,16	4,8,9	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	3,10,17	4,8,9,15,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	3,10,16,18	4,8,9,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	3,10,14	4,8,9	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	3,10,14,16,17,18	4,8,9,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	3,10,14,18	4,8,9,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	3,10,14,16,17	4,8,9,15,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	3,10,17	4,8,9,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	3,10,16,18	4,8,9,13,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	3,10,17,18	4,8,9,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	3,10,16	4,8,9,13,15	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	3,10,14,18	4,8,9,13,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	3,10,14,16,17	4,8,9,13,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	3,10,14	4,8,9,13,15	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	3,10,14,16,17,18	4,8,9,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	3,10,12	4,8,9	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	3,10,12,16,17,18	4,8,9,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	3,10,12,18	4,8,9,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	3,10,12,16,17	4,8,9,15,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,10,12,14,17,18	4,8,9,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	3,10,12,14,16	4,8,9	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	3,10,12,14,17	4,8,9,15,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	3,10,12,14,16,18	4,8,9,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	3,10,12,18	4,8,9,13,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	3,10,12,16,17	4,8,9,13,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	3,10,12	4,8,9,13,15	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	3,10,12,16,17,18	4,8,9,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	3,10,12,14,17	4,8,9,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	3,10,12,14,16,18	4,8,9,13,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	3,10,12,14,17,18	4,8,9,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	3,10,12,14,16	4,8,9,13,15	2^{-23}

Table 0.400 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	3,10,17	4,8,9,11,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	3,10,16,18	4,8,9,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	3,10,17,18	4,8,9,11,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	3,10,16	4,8,9,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	3,10,14,18	4,8,9,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	3,10,14,16,17	4,8,9,11,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	3,10,14	4,8,9,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	3,10,14,16,17,18	4,8,9,11,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	3,10,17,18	4,8,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	3,10,16	4,8,9,11,13	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	3,10,17	4,8,9,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	3,10,16,18	4,8,9,11,13,15,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	3,10,14	4,8,9,11,13	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	3,10,14,16,17,18	4,8,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	3,10,14,18	4,8,9,11,13,15,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	3,10,14,16,17	4,8,9,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	3,10,12,18	4,8,9,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	3,10,12,16,17	4,8,9,11,17	2^{-1}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	3,10,12	4,8,9,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	3,10,12,16,17,18	4,8,9,11,15,17,18	2^{-1}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	3,10,12,14,17	4,8,9,11,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	3,10,12,14,16,18	4,8,9,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	3,10,12,14,17,18	4,8,9,11,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	3,10,12,14,16	4,8,9,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	3,10,12	4,8,9,11,13	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	3,10,12,16,17,18	4,8,9,11,13,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	3,10,12,18	4,8,9,11,13,15,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	3,10,12,16,17	4,8,9,11,13,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	3,10,12,14,17,18	4,8,9,11,13,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	3,10,12,14,16	4,8,9,11,13	2^{-12}
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	3,10,12,14,17	4,8,9,11,13,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	3,10,12,14,16,18	4,8,9,11,13,15,18	2^{-12}

Table 0.401 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	3,7,17,18	4,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	3,7,16	4	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	3,7,17	4,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	3,7,16,18	4,15,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	3,7,14	4	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	3,7,14,16,17,18	4,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	3,7,14,18	4,15,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	3,7,14,16,17	4,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	3,7,17	4,13,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	3,7,16,18	4,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	3,7,17,18	4,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	3,7,16	4,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	3,7,14,18	4,13,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	3,7,14,16,17	4,13,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	3,7,14	4,13,15	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,7,14,16,17,18	4,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	3,7,12	4	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	3,7,12,16,17,18	4,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	3,7,12,18	4,15,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	3,7,12,16,17	4,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	3,7,12,14,17,18	4,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	3,7,12,14,16	4	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	3,7,12,14,17	4,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	3,7,12,14,16,18	4,15,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	3,7,12,18	4,13,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	3,7,12,16,17	4,13,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	3,7,12	4,13,15	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	3,7,12,16,17,18	4,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	3,7,12,14,17	4,13,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	3,7,12,14,16,18	4,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	3,7,12,14,17,18	4,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	3,7,12,14,16	4,13,15	$2^{-17.5}$

Table 0.402 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	3,7,17	4,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	3,7,16,18	4,11,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	3,7,17,18	4,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	3,7,16	4,11,15	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	3,7,14,18	4,11,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	3,7,14,16,17	4,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	3,7,14	4,11,15	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	3,7,14,16,17,18	4,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	3,7,17,18	4,11,13,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	3,7,16	4,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	3,7,17	4,11,13,15,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	3,7,16,18	4,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	3,7,14	4,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	3,7,14,16,17,18	4,11,13,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	3,7,14,18	4,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	3,7,14,16,17	4,11,13,15,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	3,7,12,18	4,11,18	2^{-1}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	3,7,12,16,17	4,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	3,7,12	4,11,15	2^{-1}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	3,7,12,16,17,18	4,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	3,7,12,14,17	4,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	3,7,12,14,16,18	4,11,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	3,7,12,14,17,18	4,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	3,7,12,14,16	4,11,15	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	3,7,12	4,11,13	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	3,7,12,16,17,18	4,11,13,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	3,7,12,18	4,11,13,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	3,7,12,16,17	4,11,13,15,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	3,7,12,14,17,18	4,11,13,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	3,7,12,14,16	4,11,13	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	3,7,12,14,17	4,11,13,15,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	3,7,12,14,16,18	4,11,13,15,18	$2^{-6.5}$

Table 0.403 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	3,7,10	4	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	3,7,10,16,17,18	4,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	3,7,10,18	4,15,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	3,7,10,16,17	4,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	3,7,10,14,17,18	4,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	3,7,10,14,16	4	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	3,7,10,14,17	4,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	3,7,10,14,16,18	4,15,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	3,7,10,18	4,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	3,7,10,16,17	4,13,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	3,7,10	4,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	3,7,10,16,17,18	4,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	3,7,10,14,17	4,13,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	3,7,10,14,16,18	4,13,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,7,10,14,17,18	4,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	3,7,10,14,16	4,13,15	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	3,7,10,12,17,18	4,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	3,7,10,12,16	4	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	3,7,10,12,17	4,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	3,7,10,12,16,18	4,15,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	3,7,10,12,14	4	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,7,10,12,14,16,17,18	4,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	3,7,10,12,14,18	4,15,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	3,7,10,12,14,16,17	4,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	3,7,10,12,17	4,13,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	3,7,10,12,16,18	4,13,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	3,7,10,12,17,18	4,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	3,7,10,12,16	4,13,15	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	3,7,10,12,14,18	4,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	3,7,10,12,14,16,17	4,13,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	3,7,10,12,14	4,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	3,7,10,12,14,16,17,18	4,13,15,17,18	2^{-12}

Table 0.404 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	3,7,10,18	4,11,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	3,7,10,16,17	4,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	3,7,10	4,11,15	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	3,7,10,16,17,18	4,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	3,7,10,14,17	4,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	3,7,10,14,16,18	4,11,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	3,7,10,14,17,18	4,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	3,7,10,14,16	4,11,15	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	3,7,10	4,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	3,7,10,16,17,18	4,11,13,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	3,7,10,18	4,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	3,7,10,16,17	4,11,13,15,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	3,7,10,14,17,18	4,11,13,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	3,7,10,14,16	4,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	3,7,10,14,17	4,11,13,15,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	3,7,10,14,16,18	4,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	3,7,10,12,17	4,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	3,7,10,12,16,18	4,11,18	2^{-34}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	3,7,10,12,17,18	4,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	3,7,10,12,16	4,11,15	2^{-34}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	3,7,10,12,14,18	4,11,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	3,7,10,12,14,16,17	4,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	3,7,10,12,14	4,11,15	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	3,7,10,12,14,16,17,18	4,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	3,7,10,12,17,18	4,11,13,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	3,7,10,12,16	4,11,13	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	3,7,10,12,17	4,11,13,15,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	3,7,10,12,16,18	4,11,13,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	3,7,10,12,14	4,11,13	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	3,7,10,12,14,16,17,18	4,11,13,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	3,7,10,12,14,18	4,11,13,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	3,7,10,12,14,16,17	4,11,13,15,17	2^{-23}

Table 0.405 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	3,7,17	4,9,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	3,7,16,18	4,9,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	3,7,17,18	4,9,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	3,7,16	4,9,15	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	3,7,14,18	4,9,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	3,7,14,16,17	4,9,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	3,7,14	4,9,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	3,7,14,16,17,18	4,9,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	3,7,17,18	4,9,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	3,7,16	4,9,13	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	3,7,17	4,9,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	3,7,16,18	4,9,13,15,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	3,7,14	4,9,13	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	3,7,14,16,17,18	4,9,13,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	3,7,14,18	4,9,13,15,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	3,7,14,16,17	4,9,13,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	3,7,12,18	4,9,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	3,7,12,16,17	4,9,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	3,7,12	4,9,15	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	3,7,12,16,17,18	4,9,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	3,7,12,14,17	4,9,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	3,7,12,14,16,18	4,9,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	3,7,12,14,17,18	4,9,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	3,7,12,14,16	4,9,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	3,7,12	4,9,13	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	3,7,12,16,17,18	4,9,13,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	3,7,12,18	4,9,13,15,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	3,7,12,16,17	4,9,13,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	3,7,12,14,17,18	4,9,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	3,7,12,14,16	4,9,13	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	3,7,12,14,17	4,9,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	3,7,12,14,16,18	4,9,13,15,18	2^{-12}

Table 0.406 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	3,7,17,18	4,9,11,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	3,7,16	4,9,11	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	3,7,17	4,9,11,15,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	3,7,16,18	4,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	3,7,14	4,9,11	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	3,7,14,16,17,18	4,9,11,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	3,7,14,18	4,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	3,7,14,16,17	4,9,11,15,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	3,7,17	4,9,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	3,7,16,18	4,9,11,13,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	3,7,17,18	4,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	3,7,16	4,9,11,13,15	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	3,7,14,18	4,9,11,13,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	3,7,14,16,17	4,9,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	3,7,16,18	4,9,11,13,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	3,7,17,18	4,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	3,7,16	4,9,11,13,15	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	3,7,14,18	4,9,11,13,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	3,7,14,16,17	4,9,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	3,7,14	4,9,11,13,15	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	3,7,14,16,17,18	4,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	3,7,12	4,9,11	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	3,7,12,16,17,18	4,9,11,17,18	2^{-34}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	3,7,12,18	4,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	3,7,12,16,17	4,9,11,15,17	2^{-34}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	3,7,12,14,17,18	4,9,11,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	3,7,12,14,16	4,9,11	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	3,7,12,14,17	4,9,11,15,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,7,12,14,16,18	4,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	3,7,12,18	4,9,11,13,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	3,7,12,16,17	4,9,11,13,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	3,7,12	4,9,11,13,15	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	3,7,12,16,17,18	4,9,11,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	3,7,12,14,17	4,9,11,13,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	3,7,12,14,16,18	4,9,11,13,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	3,7,12,14,17,18	4,9,11,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	3,7,12,14,16	4,9,11,13,15	2^{-23}

Table 0.407 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	3,7,10,18	4,9,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	3,7,10,16,17	4,9,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	3,7,10	4,9,15	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	3,7,10,16,17,18	4,9,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	3,7,10,14,17	4,9,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	3,7,10,14,16,18	4,9,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	3,7,10,14,17,18	4,9,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	3,7,10,14,16	4,9,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	3,7,10	4,9,13	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	3,7,10,16,17,18	4,9,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	3,7,10,18	4,9,13,15,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	3,7,10,16,17	4,9,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	3,7,10,14,17,18	4,9,13,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	3,7,10,14,16	4,9,13	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	3,7,10,14,17	4,9,13,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	3,7,10,14,16,18	4,9,13,15,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	3,7,10,12,17	4,9,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	3,7,10,12,16,18	4,9,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	3,7,10,12,17,18	4,9,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	3,7,10,12,16	4,9,15	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	3,7,10,12,14,18	4,9,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	3,7,10,12,14,16,17	4,9,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	3,7,10,12,14	4,9,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	3,7,10,12,14,16,17,18	4,9,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	3,7,10,12,17,18	4,9,13,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	3,7,10,12,16	4,9,13	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	3,7,10,12,17	4,9,13,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	3,7,10,12,16,18	4,9,13,15,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	3,7,10,12,14	4,9,13	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	3,7,10,12,14,16,17,18	4,9,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	3,7,10,12,14,18	4,9,13,15,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	3,7,10,12,14,16,17	4,9,13,15,17	$2^{-17.5}$

Table 0.408 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	3,7,10	4,9,11	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	3,7,10,16,17,18	4,9,11,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	3,7,10,18	4,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	3,7,10,16,17	4,9,11,15,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	3,7,10,14,17,18	4,9,11,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	3,7,10,14,16	4,9,11	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,7,10,14,17	4,9,11,15,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	3,7,10,14,16,18	4,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	3,7,10,18	4,9,11,13,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	3,7,10,16,17	4,9,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	3,7,10	4,9,11,13,15	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	3,7,10,16,17,18	4,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	3,7,10,14,17	4,9,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	3,7,10,14,16,18	4,9,11,13,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,7,10,14,17,18	4,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,7,10,14,16	4,9,11,13,15	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	3,7,10,12,17,18	4,9,11,17,18	2^{-1}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	3,7,10,12,16	4,9,11	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	3,7,10,12,17	4,9,11,15,17	2^{-1}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	3,7,10,12,16,18	4,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	3,7,10,12,14	4,9,11	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	3,7,10,12,14,16,17,18	4,9,11,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	3,7,10,12,14,18	4,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	3,7,10,12,14,16,17	4,9,11,15,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	3,7,10,12,17	4,9,11,13,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	3,7,10,12,16,18	4,9,11,13,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	3,7,10,12,17,18	4,9,11,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	3,7,10,12,16	4,9,11,13,15	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	3,7,10,12,14,18	4,9,11,13,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	3,7,10,12,14,16,17	4,9,11,13,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	3,7,10,12,14	4,9,11,13,15	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	3,7,10,12,14,16,17,18	4,9,11,13,15,17,18	$2^{-6.5}$

Table 0.409 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	3,7	4,8	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	3,7,16,17,18	4,8,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	3,7,18	4,8,15,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	3,7,16,17	4,8,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	3,7,14,17,18	4,8,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	3,7,14,16	4,8	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	3,7,14,17	4,8,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	3,7,14,16,18	4,8,15,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	3,7,18	4,8,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	3,7,16,17	4,8,13,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	3,7	4,8,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	3,7,16,17,18	4,8,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	3,7,14,17	4,8,13,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	3,7,14,16,18	4,8,13,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	3,7,14,17,18	4,8,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	3,7,14,16	4,8,13,15	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	3,7,12,17,18	4,8,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	3,7,12,16	4,8	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	3,7,12,17	4,8,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	3,7,12,16,18	4,8,15,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	3,7,12,14	4,8	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	3,7,12,14,16,17,18	4,8,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	3,7,12,14,18	4,8,15,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	3,7,12,14,16,17	4,8,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	3,7,12,17	4,8,13,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	3,7,12,16,18	4,8,13,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	3,7,12,17,18	4,8,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	3,7,12,16	4,8,13,15	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	3,7,12,14,18	4,8,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	3,7,12,14,16,17	4,8,13,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	3,7,12,14	4,8,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	3,7,12,14,16,17,18	4,8,13,15,17,18	2^{-23}

Table 0.410 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	3,7,18	4,8,11,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	3,7,16,17	4,8,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	3,7	4,8,11,15	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	3,7,16,17,18	4,8,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	3,7,14,17	4,8,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	3,7,14,16,18	4,8,11,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	3,7,14,17,18	4,8,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,7,14,16	4,8,11,15	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	3,7	4,8,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	3,7,16,17,18	4,8,11,13,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	3,7,18	4,8,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	3,7,16,17	4,8,11,13,15,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	3,7,14,17,18	4,8,11,13,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	3,7,14,16	4,8,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,7,14,17	4,8,11,13,15,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,7,14,16,18	4,8,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	3,7,12,17	4,8,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	3,7,12,16,18	4,8,11,18	2^{-1}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	3,7,12,17,18	4,8,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	3,7,12,16	4,8,11,15	2^{-1}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	3,7,12,14,18	4,8,11,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	3,7,12,14,16,17	4,8,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	3,7,12,14	4,8,11,15	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	3,7,12,14,16,17,18	4,8,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	3,7,12,17,18	4,8,11,13,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	3,7,12,16	4,8,11,13	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	3,7,12,17	4,8,11,13,15,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	3,7,12,16,18	4,8,11,13,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	3,7,12,14	4,8,11,13	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	3,7,12,14,16,17,18	4,8,11,13,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	3,7,12,14,18	4,8,11,13,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	3,7,12,14,16,17	4,8,11,13,15,17	2^{-12}

Table 0.411 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	3,7,10,17,18	4,8,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	3,7,10,16	4,8	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	3,7,10,17	4,8,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	3,7,10,16,18	4,8,15,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	3,7,10,14	4,8	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	3,7,10,14,16,17,18	4,8,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	3,7,10,14,18	4,8,15,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	3,7,10,14,16,17	4,8,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	3,7,10,17	4,8,13,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	3,7,10,16,18	4,8,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	3,7,10,17,18	4,8,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	3,7,10,16	4,8,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	3,7,10,14,18	4,8,13,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	3,7,10,14,16,17	4,8,13,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	3,7,10,14	4,8,13,15	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	3,7,10,14,16,17,18	4,8,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	3,7,10,12	4,8	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	3,7,10,12,16,17,18	4,8,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	3,7,10,12,18	4,8,15,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	3,7,10,12,16,17	4,8,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	3,7,10,12,14,17,18	4,8,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	3,7,10,12,14,16	4,8	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	3,7,10,12,14,17	4,8,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	3,7,10,12,14,16,18	4,8,15,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	3,7,10,12,18	4,8,13,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	3,7,10,12,16,17	4,8,13,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	3,7,10,12	4,8,13,15	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	3,7,10,12,16,17,18	4,8,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	3,7,10,12,14,17	4,8,13,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	3,7,10,12,14,16,18	4,8,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	3,7,10,12,14,17,18	4,8,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	3,7,10,12,14,16	4,8,13,15	$2^{-17.5}$

Table 0.412 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	3,7,10,17	4,8,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	3,7,10,16,18	4,8,11,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	3,7,10,17,18	4,8,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	3,7,10,16	4,8,11,15	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	3,7,10,14,18	4,8,11,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	3,7,10,14,16,17	4,8,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	3,7,10,14	4,8,11,15	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	3,7,10,14,16,17,18	4,8,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	3,7,10,17,18	4,8,11,13,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	3,7,10,16	4,8,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	3,7,10,17	4,8,11,13,15,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	3,7,10,16,18	4,8,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	3,7,10,14	4,8,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	3,7,10,14,16,17,18	4,8,11,13,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	3,7,10,14,18	4,8,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	3,7,10,14,16,17	4,8,11,13,15,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	3,7,10,12,18	4,8,11,18	2^{-34}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	3,7,10,12,16,17	4,8,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	3,7,10,12	4,8,11,15	2^{-34}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	3,7,10,12,16,17,18	4,8,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	3,7,10,12,14,17	4,8,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	3,7,10,12,14,16,18	4,8,11,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,7,10,12,14,17,18	4,8,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	3,7,10,12,14,16	4,8,11,15	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	3,7,10,12	4,8,11,13	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	3,7,10,12,16,17,18	4,8,11,13,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	3,7,10,12,18	4,8,11,13,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	3,7,10,12,16,17	4,8,11,13,15,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	3,7,10,12,14,17,18	4,8,11,13,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	3,7,10,12,14,16	4,8,11,13	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	3,7,10,12,14,17	4,8,11,13,15,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	3,7,10,12,14,16,18	4,8,11,13,15,18	$2^{-28.5}$

Table 0.413 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	3,7,18	4,8,9,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	3,7,16,17	4,8,9,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	3,7	4,8,9,15	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	3,7,16,17,18	4,8,9,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	3,7,14,17	4,8,9,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	3,7,14,16,18	4,8,9,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	3,7,14,17,18	4,8,9,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	3,7,14,16	4,8,9,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	3,7	4,8,9,13	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	3,7,16,17,18	4,8,9,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	3,7,18	4,8,9,13,15,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	3,7,16,17	4,8,9,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	3,7,14,17,18	4,8,9,13,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	3,7,14,16	4,8,9,13	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	3,7,14,17	4,8,9,13,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,7,14,16,18	4,8,9,13,15,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	3,7,12,17	4,8,9,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	3,7,12,16,18	4,8,9,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	3,7,12,17,18	4,8,9,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	3,7,12,16	4,8,9,15	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,7,12,14,18	4,8,9,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	3,7,12,14,16,17	4,8,9,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	3,7,12,14	4,8,9,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	3,7,12,14,16,17,18	4,8,9,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	3,7,12,17,18	4,8,9,13,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	3,7,12,16	4,8,9,13	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	3,7,12,17	4,8,9,13,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	3,7,12,16,18	4,8,9,13,15,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	3,7,12,14	4,8,9,13	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	3,7,12,14,16,17,18	4,8,9,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	3,7,12,14,18	4,8,9,13,15,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	3,7,12,14,16,17	4,8,9,13,15,17	$2^{-17.5}$

Table 0.414 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	3,7	4,8,9,11	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	3,7,16,17,18	4,8,9,11,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	3,7,18	4,8,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	3,7,16,17	4,8,9,11,15,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	3,7,14,17,18	4,8,9,11,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	3,7,14,16	4,8,9,11	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	3,7,14,17	4,8,9,11,15,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	3,7,14,16,18	4,8,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	3,7,18	4,8,9,11,13,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	3,7,16,17	4,8,9,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	3,7	4,8,9,11,13,15	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	3,7,16,17,18	4,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	3,7,14,17	4,8,9,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	3,7,14,16,18	4,8,9,11,13,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,7,14,17,18	4,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	3,7,14,16	4,8,9,11,13,15	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	3,7,12,17,18	4,8,9,11,17,18	2^{-34}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	3,7,12,16	4,8,9,11	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	3,7,12,17	4,8,9,11,15,17	2^{-34}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	3,7,12,16,18	4,8,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	3,7,12,14	4,8,9,11	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	3,7,12,14,16,17,18	4,8,9,11,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	3,7,12,14,18	4,8,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	3,7,12,14,16,17	4,8,9,11,15,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	3,7,12,17	4,8,9,11,13,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	3,7,12,16,18	4,8,9,11,13,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	3,7,12,17,18	4,8,9,11,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	3,7,12,16	4,8,9,11,13,15	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	3,7,12,14,18	4,8,9,11,13,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	3,7,12,14,16,17	4,8,9,11,13,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	3,7,12,14	4,8,9,11,13,15	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	3,7,12,14,16,17,18	4,8,9,11,13,15,17,18	$2^{-28.5}$

Table 0.415 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	3,7,10,17	4,8,9,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	3,7,10,16,18	4,8,9,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	3,7,10,17,18	4,8,9,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	3,7,10,16	4,8,9,15	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	3,7,10,14,18	4,8,9,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	3,7,10,14,16,17	4,8,9,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	3,7,10,14	4,8,9,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	3,7,10,14,16,17,18	4,8,9,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	3,7,10,17,18	4,8,9,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	3,7,10,16	4,8,9,13	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	3,7,10,17	4,8,9,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	3,7,10,16,18	4,8,9,13,15,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	3,7,10,14	4,8,9,13	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	3,7,10,14,16,17,18	4,8,9,13,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,7,10,14,18	4,8,9,13,15,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	3,7,10,14,16,17	4,8,9,13,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	3,7,10,12,18	4,8,9,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	3,7,10,12,16,17	4,8,9,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	3,7,10,12	4,8,9,15	$2^{-28.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	3,7,10,12,16,17,18	4,8,9,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	3,7,10,12,14,17	4,8,9,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	3,7,10,12,14,16,18	4,8,9,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	3,7,10,12,14,17,18	4,8,9,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	3,7,10,12,14,16	4,8,9,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	3,7,10,12	4,8,9,13	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	3,7,10,12,16,17,18	4,8,9,13,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	3,7,10,12,18	4,8,9,13,15,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	3,7,10,12,16,17	4,8,9,13,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	3,7,10,12,14,17,18	4,8,9,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	3,7,10,12,14,16	4,8,9,13	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	3,7,10,12,14,17	4,8,9,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	3,7,10,12,14,16,18	4,8,9,13,15,18	2^{-23}

Table 0.416 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	3,7,10,17,18	4,8,9,11,17,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	3,7,10,16	4,8,9,11	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	3,7,10,17	4,8,9,11,15,17	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	3,7,10,16,18	4,8,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	3,7,10,14	4,8,9,11	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	3,7,10,14,16,17,18	4,8,9,11,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	3,7,10,14,18	4,8,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	3,7,10,14,16,17	4,8,9,11,15,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	3,7,10,17	4,8,9,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	3,7,10,16,18	4,8,9,11,13,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	3,7,10,17,18	4,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	3,7,10,16	4,8,9,11,13,15	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	3,7,10,14,18	4,8,9,11,13,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	3,7,10,14,16,17	4,8,9,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	3,7,10,14	4,8,9,11,13,15	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	3,7,10,14,16,17,18	4,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	3,7,10,12	4,8,9,11	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	3,7,10,12,16,17,18	4,8,9,11,17,18	2^{-1}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	3,7,10,12,18	4,8,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	3,7,10,12,16,17	4,8,9,11,15,17	2^{-1}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	3,7,10,12,14,17,18	4,8,9,11,17,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	3,7,10,12,14,16	4,8,9,11	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	3,7,10,12,14,17	4,8,9,11,15,17	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	3,7,10,12,14,16,18	4,8,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	3,7,10,12,18	4,8,9,11,13,18	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	3,7,10,12,16,17	4,8,9,11,13,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	3,7,10,12	4,8,9,11,13,15	2^{-23}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	3,7,10,12,16,17,18	4,8,9,11,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	3,7,10,12,14,17	4,8,9,11,13,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	3,7,10,12,14,16,18	4,8,9,11,13,18	2^{-12}
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	3,7,10,12,14,17,18	4,8,9,11,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	3,7,10,12,14,16	4,8,9,11,13,15	2^{-12}

Table 0.417 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	3,18	4,6,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	3,16,17	4,6,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	3	4,6,15	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	3,16,17,18	4,6,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	3,14,17	4,6,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	3,14,16,18	4,6,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	3,14,17,18	4,6,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	3,14,16	4,6,15	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	3	4,6,13	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	3,16,17,18	4,6,13,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	3,18	4,6,13,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	3,16,17	4,6,13,15,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	3,14,17,18	4,6,13,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	3,14,16	4,6,13	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	3,14,17	4,6,13,15,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	3,14,16,18	4,6,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,12,17	4,6,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	3,12,16,18	4,6,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	3,12,17,18	4,6,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	3,12,16	4,6,15	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	3,12,14,18	4,6,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	3,12,14,16,17	4,6,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	3,12,14	4,6,15	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	3,12,14,16,17,18	4,6,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,12,17,18	4,6,13,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,12,16	4,6,13	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	3,12,17	4,6,13,15,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	3,12,16,18	4,6,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	3,12,14	4,6,13	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	3,12,14,16,17,18	4,6,13,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	3,12,14,18	4,6,13,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	3,12,14,16,17	4,6,13,15,17	2^{-23}

Table 0.418 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	3	4,6,11	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	3,16,17,18	4,6,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	3,18	4,6,11,15,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	3,16,17	4,6,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	3,14,17,18	4,6,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	3,14,16	4,6,11	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	3,14,17	4,6,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	3,14,16,18	4,6,11,15,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	3,18	4,6,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	3,16,17	4,6,11,13,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	3	4,6,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	3,16,17,18	4,6,11,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	3,14,17	4,6,11,13,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	3,14,16,18	4,6,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	3,14,17,18	4,6,11,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	3,14,16	4,6,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	3,12,17,18	4,6,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	3,12,16	4,6,11	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	3,12,17	4,6,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	3,12,16,18	4,6,11,15,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	3,12,14	4,6,11	2^{-1}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	3,12,14,16,17,18	4,6,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	3,12,14,18	4,6,11,15,18	2^{-1}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	3,12,14,16,17	4,6,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	3,12,17	4,6,11,13,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	3,12,16,18	4,6,11,13,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	3,12,17,18	4,6,11,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	3,12,16	4,6,11,13,15	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	3,12,14,18	4,6,11,13,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	3,12,14,16,17	4,6,11,13,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	3,12,14	4,6,11,13,15	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	3,12,14,16,17,18	4,6,11,13,15,17,18	2^{-23}

Table 0.419 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(2)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	3,10,17	4,6,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,10,16,18	4,6,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	3,10,17,18	4,6,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	3,10,16	4,6,15	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	3,10,14,18	4,6,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	3,10,14,16,17	4,6,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	3,10,14	4,6,15	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	3,10,14,16,17,18	4,6,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	3,10,17,18	4,6,13,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	3,10,16	4,6,13	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	3,10,17	4,6,13,15,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	3,10,16,18	4,6,13,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	3,10,14	4,6,13	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	3,10,14,16,17,18	4,6,13,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	3,10,14,18	4,6,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	3,10,14,16,17	4,6,13,15,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	3,10,12,18	4,6,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	3,10,12,16,17	4,6,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	3,10,12	4,6,15	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	3,10,12,16,17,18	4,6,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	3,10,12,14,17	4,6,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	3,10,12,14,16,18	4,6,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	3,10,12,14,17,18	4,6,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	3,10,12,14,16	4,6,15	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	3,10,12	4,6,13	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	3,10,12,16,17,18	4,6,13,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	3,10,12,18	4,6,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	3,10,12,16,17	4,6,13,15,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	3,10,12,14,17,18	4,6,13,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	3,10,12,14,16	4,6,13	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	3,10,12,14,17	4,6,13,15,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	3,10,12,14,16,18	4,6,13,15,18	$2^{-28.5}$

Table 0.420 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	3,10,17,18	4,6,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	3,10,16	4,6,11	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	3,10,17	4,6,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	3,10,16,18	4,6,11,15,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	3,10,14	4,6,11	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	3,10,14,16,17,18	4,6,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	3,10,14,18	4,6,11,15,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	3,10,14,16,17	4,6,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	3,10,17	4,6,11,13,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	3,10,16,18	4,6,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	3,10,17,18	4,6,11,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	3,10,16	4,6,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	3,10,14,18	4,6,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	3,10,14,16,17	4,6,11,13,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	3,10,14	4,6,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	3,10,14,16,17,18	4,6,11,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	3,10,12	4,6,11	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	3,10,12,16,17,18	4,6,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	3,10,12,18	4,6,11,15,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	3,10,12,16,17	4,6,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	3,10,12,14,17,18	4,6,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	3,10,12,14,16	4,6,11	2^{-34}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	3,10,12,14,17	4,6,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	3,10,12,14,16,18	4,6,11,15,18	2^{-34}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	3,10,12,18	4,6,11,13,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	3,10,12,16,17	4,6,11,13,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	3,10,12	4,6,11,13,15	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	3,10,12,16,17,18	4,6,11,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	3,10,12,14,17	4,6,11,13,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	3,10,12,14,16,18	4,6,11,13,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	3,10,12,14,17,18	4,6,11,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	3,10,12,14,16	4,6,11,13,15	$2^{-28.5}$

Table 0.421 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	3	4,6,9	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	3,16,17,18	4,6,9,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	3,18	4,6,9,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	3,16,17	4,6,9,15,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	3,14,17,18	4,6,9,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	3,14,16	4,6,9	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	3,14,17	4,6,9,15,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	3,14,16,18	4,6,9,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	3,18	4,6,9,13,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	3,16,17	4,6,9,13,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	3	4,6,9,13,15	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	3,16,17,18	4,6,9,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	3,14,17	4,6,9,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	3,14,16,18	4,6,9,13,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	3,14,17,18	4,6,9,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	3,14,16	4,6,9,13,15	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	3,12,17,18	4,6,9,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	3,12,16	4,6,9	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	3,12,17	4,6,9,15,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	3,12,16,18	4,6,9,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	3,12,14	4,6,9	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	3,12,14,16,17,18	4,6,9,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	3,12,14,18	4,6,9,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	3,12,14,16,17	4,6,9,15,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	3,12,17	4,6,9,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	3,12,16,18	4,6,9,13,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	3,12,17,18	4,6,9,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	3,12,16	4,6,9,13,15	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	3,12,14,18	4,6,9,13,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	3,12,14,16,17	4,6,9,13,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	3,12,14	4,6,9,13,15	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	3,12,14,16,17,18	4,6,9,13,15,17,18	$2^{-28.5}$

Table 0.422 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	3,18	4,6,9,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	3,16,17	4,6,9,11,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	3	4,6,9,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	3,16,17,18	4,6,9,11,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	3,14,17	4,6,9,11,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	3,14,16,18	4,6,9,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	3,14,17,18	4,6,9,11,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	3,14,16	4,6,9,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	3	4,6,9,11,13	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	3,16,17,18	4,6,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	3,18	4,6,9,11,13,15,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	3,16,17	4,6,9,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	3,14,17,18	4,6,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	3,14,16	4,6,9,11,13	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	3,14,17	4,6,9,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	3,14,16,18	4,6,9,11,13,15,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	3,12,17	4,6,9,11,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	3,12,16,18	4,6,9,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	3,12,17,18	4,6,9,11,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	3,12,16	4,6,9,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	3,12,14,18	4,6,9,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	3,12,14,16,17	4,6,9,11,17	2^{-34}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	3,12,14	4,6,9,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	3,12,14,16,17,18	4,6,9,11,15,17,18	2^{-34}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,12,17,18	4,6,9,11,13,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	3,12,16	4,6,9,11,13	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	3,12,17	4,6,9,11,13,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	3,12,16,18	4,6,9,11,13,15,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	3,12,14	4,6,9,11,13	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	3,12,14,16,17,18	4,6,9,11,13,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	3,12,14,18	4,6,9,11,13,15,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	3,12,14,16,17	4,6,9,11,13,15,17	$2^{-28.5}$

Table 0.423 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	3,10,17,18	4,6,9,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	3,10,16	4,6,9	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	3,10,17	4,6,9,15,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	3,10,16,18	4,6,9,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	3,10,14	4,6,9	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	3,10,14,16,17,18	4,6,9,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	3,10,14,18	4,6,9,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	3,10,14,16,17	4,6,9,15,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	3,10,17	4,6,9,13,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	3,10,16,18	4,6,9,13,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	3,10,17,18	4,6,9,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	3,10,16	4,6,9,13,15	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	3,10,14,18	4,6,9,13,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	3,10,14,16,17	4,6,9,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	3,10,14	4,6,9,13,15	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	3,10,14,16,17,18	4,6,9,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	3,10,12	4,6,9	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	3,10,12,16,17,18	4,6,9,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	3,10,12,18	4,6,9,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	3,10,12,16,17	4,6,9,15,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	3,10,12,14,17,18	4,6,9,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	3,10,12,14,16	4,6,9	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	3,10,12,14,17	4,6,9,15,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	3,10,12,14,16,18	4,6,9,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	3,10,12,18	4,6,9,13,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	3,10,12,16,17	4,6,9,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	3,10,12	4,6,9,13,15	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	3,10,12,16,17,18	4,6,9,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	3,10,12,14,17	4,6,9,13,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	3,10,12,14,16,18	4,6,9,13,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	3,10,12,14,17,18	4,6,9,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	3,10,12,14,16	4,6,9,13,15	2^{-23}

Table 0.424 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	3,10,17	4,6,9,11,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	3,10,16,18	4,6,9,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	3,10,17,18	4,6,9,11,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	3,10,16	4,6,9,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	3,10,14,18	4,6,9,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	3,10,14,16,17	4,6,9,11,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	3,10,14	4,6,9,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	3,10,14,16,17,18	4,6,9,11,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	3,10,17,18	4,6,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	3,10,16	4,6,9,11,13	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	3,10,17	4,6,9,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	3,10,16,18	4,6,9,11,13,15,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	3,10,14	4,6,9,11,13	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	3,10,14,16,17,18	4,6,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	3,10,14,18	4,6,9,11,13,15,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	3,10,14,16,17	4,6,9,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	3,10,12,18	4,6,9,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	3,10,12,16,17	4,6,9,11,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	3,10,12	4,6,9,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	3,10,12,16,17,18	4,6,9,11,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	3,10,12,14,17	4,6,9,11,17	2^{-1}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	3,10,12,14,16,18	4,6,9,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	3,10,12,14,17,18	4,6,9,11,15,17,18	2^{-1}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	3,10,12,14,16	4,6,9,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	3,10,12	4,6,9,11,13	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,10,12,16,17,18	4,6,9,11,13,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	3,10,12,18	4,6,9,11,13,15,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	3,10,12,16,17	4,6,9,11,13,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	3,10,12,14,17,18	4,6,9,11,13,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	3,10,12,14,16	4,6,9,11,13	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	3,10,12,14,17	4,6,9,11,13,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	3,10,12,14,16,18	4,6,9,11,13,15,18	2^{-23}

Table 0.425 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	3,17	4,6,8,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	3,16,18	4,6,8,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	3,17,18	4,6,8,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	3,16	4,6,8,15	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	3,14,18	4,6,8,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	3,14,16,17	4,6,8,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	3,14	4,6,8,15	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	3,14,16,17,18	4,6,8,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	3,17,18	4,6,8,13,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	3,16	4,6,8,13	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	3,17	4,6,8,13,15,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	3,16,18	4,6,8,13,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	3,14	4,6,8,13	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	3,14,16,17,18	4,6,8,13,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	3,14,18	4,6,8,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	3,14,16,17	4,6,8,13,15,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	3,12,18	4,6,8,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	3,12,16,17	4,6,8,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	3,12	4,6,8,15	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	3,12,16,17,18	4,6,8,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	3,12,14,17	4,6,8,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	3,12,14,16,18	4,6,8,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	3,12,14,17,18	4,6,8,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	3,12,14,16	4,6,8,15	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	3,12	4,6,8,13	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	3,12,16,17,18	4,6,8,13,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	3,12,18	4,6,8,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	3,12,16,17	4,6,8,13,15,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	3,12,14,17,18	4,6,8,13,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	3,12,14,16	4,6,8,13	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	3,12,14,17	4,6,8,13,15,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	3,12,14,16,18	4,6,8,13,15,18	$2^{-6.5}$

Table 0.426 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	3,17,18	4,6,8,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	3,16	4,6,8,11	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	3,17	4,6,8,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	3,16,18	4,6,8,11,15,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	3,14	4,6,8,11	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	3,14,16,17,18	4,6,8,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	3,14,18	4,6,8,11,15,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	3,14,16,17	4,6,8,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	3,17	4,6,8,11,13,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	3,16,18	4,6,8,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	3,17,18	4,6,8,11,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	3,16	4,6,8,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	3,14,18	4,6,8,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	3,14,16,17	4,6,8,11,13,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	3,14	4,6,8,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	3,14,16,17,18	4,6,8,11,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	3,12	4,6,8,11	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	3,12,16,17,18	4,6,8,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	3,12,18	4,6,8,11,15,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	3,12,16,17	4,6,8,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	3,12,14,17,18	4,6,8,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	3,12,14,16	4,6,8,11	2^{-1}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	3,12,14,17	4,6,8,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	3,12,14,16,18	4,6,8,11,15,18	2^{-1}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,12,18	4,6,8,11,13,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	3,12,16,17	4,6,8,11,13,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	3,12	4,6,8,11,13,15	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	3,12,16,17,18	4,6,8,11,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	3,12,14,17	4,6,8,11,13,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	3,12,14,16,18	4,6,8,11,13,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	3,12,14,17,18	4,6,8,11,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	3,12,14,16	4,6,8,11,13,15	$2^{-6.5}$

Table 0.427 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	3,10,18	4,6,8,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	3,10,16,17	4,6,8,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	3,10	4,6,8,15	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	3,10,16,17,18	4,6,8,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	3,10,14,17	4,6,8,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	3,10,14,16,18	4,6,8,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	3,10,14,17,18	4,6,8,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	3,10,14,16	4,6,8,15	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	3,10	4,6,8,13	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	3,10,16,17,18	4,6,8,13,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	3,10,18	4,6,8,13,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	3,10,16,17	4,6,8,13,15,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	3,10,14,17,18	4,6,8,13,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	3,10,14,16	4,6,8,13	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	3,10,14,17	4,6,8,13,15,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	3,10,14,16,18	4,6,8,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	3,10,12,17	4,6,8,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	3,10,12,16,18	4,6,8,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	3,10,12,17,18	4,6,8,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	3,10,12,16	4,6,8,15	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	3,10,12,14,18	4,6,8,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	3,10,12,14,16,17	4,6,8,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	3,10,12,14	4,6,8,15	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	3,10,12,14,16,17,18	4,6,8,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	3,10,12,17,18	4,6,8,13,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	3,10,12,16	4,6,8,13	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	3,10,12,17	4,6,8,13,15,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	3,10,12,16,18	4,6,8,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	3,10,12,14	4,6,8,13	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	3,10,12,14,16,17,18	4,6,8,13,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	3,10,12,14,18	4,6,8,13,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	3,10,12,14,16,17	4,6,8,13,15,17	2^{-12}

Table 0.428 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	3,10	4,6,8,11	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	3,10,16,17,18	4,6,8,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	3,10,18	4,6,8,11,15,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	3,10,16,17	4,6,8,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	3,10,14,17,18	4,6,8,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	3,10,14,16	4,6,8,11	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	3,10,14,17	4,6,8,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	3,10,14,16,18	4,6,8,11,15,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	3,10,18	4,6,8,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	3,10,16,17	4,6,8,11,13,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	3,10	4,6,8,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	3,10,16,17,18	4,6,8,11,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	3,10,14,17	4,6,8,11,13,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	3,10,14,16,18	4,6,8,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	3,10,14,17,18	4,6,8,11,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	3,10,14,16	4,6,8,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	3,10,12,17,18	4,6,8,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	3,10,12,16	4,6,8,11	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	3,10,12,17	4,6,8,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	3,10,12,16,18	4,6,8,11,15,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	3,10,12,14	4,6,8,11	2^{-34}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	3,10,12,14,16,17,18	4,6,8,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	3,10,12,14,18	4,6,8,11,15,18	2^{-34}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	3,10,12,14,16,17	4,6,8,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	3,10,12,17	4,6,8,11,13,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,10,12,16,18	4,6,8,11,13,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	3,10,12,17,18	4,6,8,11,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	3,10,12,16	4,6,8,11,13,15	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	3,10,12,14,18	4,6,8,11,13,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	3,10,12,14,16,17	4,6,8,11,13,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	3,10,12,14	4,6,8,11,13,15	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	3,10,12,14,16,17,18	4,6,8,11,13,15,17,18	2^{-12}

Table 0.429 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,17,18	4,6,8,9,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	3,16	4,6,8,9	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	3,17	4,6,8,9,15,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	3,16,18	4,6,8,9,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	3,14	4,6,8,9	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	3,14,16,17,18	4,6,8,9,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	3,14,18	4,6,8,9,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	3,14,16,17	4,6,8,9,15,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	3,17	4,6,8,9,13,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	3,16,18	4,6,8,9,13,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	3,17,18	4,6,8,9,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	3,16	4,6,8,9,13,15	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	3,14,18	4,6,8,9,13,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	3,14,16,17	4,6,8,9,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	3,14	4,6,8,9,13,15	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	3,14,16,17,18	4,6,8,9,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	3,12	4,6,8,9	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	3,12,16,17,18	4,6,8,9,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	3,12,18	4,6,8,9,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	3,12,16,17	4,6,8,9,15,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	3,12,14,17,18	4,6,8,9,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	3,12,14,16	4,6,8,9	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	3,12,14,17	4,6,8,9,15,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	3,12,14,16,18	4,6,8,9,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	3,12,18	4,6,8,9,13,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	3,12,16,17	4,6,8,9,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	3,12	4,6,8,9,13,15	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	3,12,16,17,18	4,6,8,9,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	3,12,14,17	4,6,8,9,13,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	3,12,14,16,18	4,6,8,9,13,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	3,12,14,17,18	4,6,8,9,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	3,12,14,16	4,6,8,9,13,15	2^{-12}

Table 0.430 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	3,17	4,6,8,9,11,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	3,16,18	4,6,8,9,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	3,17,18	4,6,8,9,11,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	3,16	4,6,8,9,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	3,14,18	4,6,8,9,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	3,14,16,17	4,6,8,9,11,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	3,14	4,6,8,9,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	3,14,16,17,18	4,6,8,9,11,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	3,17,18	4,6,8,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	3,16	4,6,8,9,11,13	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	3,17	4,6,8,9,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	3,16,18	4,6,8,9,11,13,15,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	3,14	4,6,8,9,11,13	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	3,14,16,17,18	4,6,8,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	3,14,18	4,6,8,9,11,13,15,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	3,14,16,17	4,6,8,9,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	3,12,18	4,6,8,9,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	3,12,16,17	4,6,8,9,11,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	3,12	4,6,8,9,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	3,12,16,17,18	4,6,8,9,11,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	3,12,14,17	4,6,8,9,11,17	2^{-34}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	3,12,14,16,18	4,6,8,9,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	3,12,14,17,18	4,6,8,9,11,15,17,18	2^{-34}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	3,12,14,16	4,6,8,9,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	3,12	4,6,8,9,11,13	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	3,12,16,17,18	4,6,8,9,11,13,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	3,12,18	4,6,8,9,11,13,15,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	3,12,16,17	4,6,8,9,11,13,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	3,12,14,17,18	4,6,8,9,11,13,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	3,12,14,16	4,6,8,9,11,13	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	3,12,14,17	4,6,8,9,11,13,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	3,12,14,16,18	4,6,8,9,11,13,15,18	2^{-12}

Table 0.431 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	3,10	4,6,8,9	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	3,10,16,17,18	4,6,8,9,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	3,10,18	4,6,8,9,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	3,10,16,17	4,6,8,9,15,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	3,10,14,17,18	4,6,8,9,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	3,10,14,16	4,6,8,9	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	3,10,14,17	4,6,8,9,15,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	3,10,14,16,18	4,6,8,9,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	3,10,18	4,6,8,9,13,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	3,10,16,17	4,6,8,9,13,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	3,10	4,6,8,9,13,15	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	3,10,16,17,18	4,6,8,9,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	3,10,14,17	4,6,8,9,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	3,10,14,16,18	4,6,8,9,13,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	3,10,14,17,18	4,6,8,9,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	3,10,14,16	4,6,8,9,13,15	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	3,10,12,17,18	4,6,8,9,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,10,12,16	4,6,8,9	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	3,10,12,17	4,6,8,9,15,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	3,10,12,16,18	4,6,8,9,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	3,10,12,14	4,6,8,9	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	3,10,12,14,16,17,18	4,6,8,9,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	3,10,12,14,18	4,6,8,9,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	3,10,12,14,16,17	4,6,8,9,15,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,10,12,17	4,6,8,9,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,10,12,16,18	4,6,8,9,13,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	3,10,12,17,18	4,6,8,9,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	3,10,12,16	4,6,8,9,13,15	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	3,10,12,14,18	4,6,8,9,13,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	3,10,12,14,16,17	4,6,8,9,13,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	3,10,12,14	4,6,8,9,13,15	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	3,10,12,14,16,17,18	4,6,8,9,13,15,17,18	$2^{-6.5}$

Table 0.432 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	3,10,18	4,6,8,9,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	3,10,16,17	4,6,8,9,11,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	3,10	4,6,8,9,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	3,10,16,17,18	4,6,8,9,11,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	3,10,14,17	4,6,8,9,11,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	3,10,14,16,18	4,6,8,9,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	3,10,14,17,18	4,6,8,9,11,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	3,10,14,16	4,6,8,9,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	3,10	4,6,8,9,11,13	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	3,10,16,17,18	4,6,8,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	3,10,18	4,6,8,9,11,13,15,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	3,10,16,17	4,6,8,9,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	3,10,14,17,18	4,6,8,9,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	3,10,14,16	4,6,8,9,11,13	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	3,10,14,17	4,6,8,9,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	3,10,14,16,18	4,6,8,9,11,13,15,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	3,10,12,17	4,6,8,9,11,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	3,10,12,16,18	4,6,8,9,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	3,10,12,17,18	4,6,8,9,11,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	3,10,12,16	4,6,8,9,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	3,10,12,14,18	4,6,8,9,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	3,10,12,17,18	4,6,8,9,11,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	3,10,12,16	4,6,8,9,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	3,10,12,14,18	4,6,8,9,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	3,10,12,14,16,17	4,6,8,9,11,17	2^{-1}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	3,10,12,14	4,6,8,9,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	3,10,12,14,16,17,18	4,6,8,9,11,15,17,18	2^{-1}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	3,10,12,17,18	4,6,8,9,11,13,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	3,10,12,16	4,6,8,9,11,13	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	3,10,12,17	4,6,8,9,11,13,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	3,10,12,16,18	4,6,8,9,11,13,15,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	3,10,12,14	4,6,8,9,11,13	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	3,10,12,14,16,17,18	4,6,8,9,11,13,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	3,10,12,14,18	4,6,8,9,11,13,15,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	3,10,12,14,16,17	4,6,8,9,11,13,15,17	$2^{-6.5}$

Table 0.433 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	3,7	4,6	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	3,7,16,17,18	4,6,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	3,7,18	4,6,15,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	3,7,16,17	4,6,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	3,7,14,17,18	4,6,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	3,7,14,16	4,6	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	3,7,14,17	4,6,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	3,7,14,16,18	4,6,15,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	3,7,18	4,6,13,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	3,7,16,17	4,6,13,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	3,7	4,6,13,15	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	3,7,16,17,18	4,6,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	3,7,14,17	4,6,13,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	3,7,14,16,18	4,6,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	3,7,14,17,18	4,6,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	3,7,14,16	4,6,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	3,7,12,17,18	4,6,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	3,7,12,16	4,6	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	3,7,12,17	4,6,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	3,7,12,16,18	4,6,15,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	3,7,12,14	4,6	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	3,7,12,14,16,17,18	4,6,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	3,7,12,14,18	4,6,15,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	3,7,12,14,16,17	4,6,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	3,7,12,17	4,6,13,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	3,7,12,16,18	4,6,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,7,12,17,18	4,6,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	3,7,12,16	4,6,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	3,7,12,14,18	4,6,13,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	3,7,12,14,16,17	4,6,13,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	3,7,12,14	4,6,13,15	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	3,7,12,14,16,17,18	4,6,13,15,17,18	2^{-23}

Table 0.434 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	3,7,18	4,6,11,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	3,7,16,17	4,6,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	3,7	4,6,11,15	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	3,7,16,17,18	4,6,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	3,7,14,17	4,6,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	3,7,14,16,18	4,6,11,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	3,7,14,17,18	4,6,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	3,7,14,16	4,6,11,15	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	3,7	4,6,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	3,7,16,17,18	4,6,11,13,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	3,7,18	4,6,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	3,7,16,17	4,6,11,13,15,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	3,7,14,17,18	4,6,11,13,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	3,7,14,16	4,6,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	3,7,14,17	4,6,11,13,15,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	3,7,14,16,18	4,6,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	3,7,12,17	4,6,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,7,12,16,18	4,6,11,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	3,7,12,17,18	4,6,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	3,7,12,16	4,6,11,15	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	3,7,12,14,18	4,6,11,18	2^{-1}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	3,7,12,14,16,17	4,6,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	3,7,12,14	4,6,11,15	2^{-1}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	3,7,12,14,16,17,18	4,6,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	3,7,12,17,18	4,6,11,13,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	3,7,12,16	4,6,11,13	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	3,7,12,17	4,6,11,13,15,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	3,7,12,16,18	4,6,11,13,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	3,7,12,14	4,6,11,13	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	3,7,12,14,16,17,18	4,6,11,13,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	3,7,12,14,18	4,6,11,13,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	3,7,12,14,16,17	4,6,11,13,15,17	2^{-23}

Table 0.435 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	3,7,10,17,18	4,6,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	3,7,10,16	4,6	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	3,7,10,17	4,6,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	3,7,10,16,18	4,6,15,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	3,7,10,14	4,6	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	3,7,10,14,16,17,18	4,6,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	3,7,10,14,18	4,6,15,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	3,7,10,14,16,17	4,6,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	3,7,10,17	4,6,13,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,7,10,16,18	4,6,13,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	3,7,10,17,18	4,6,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	3,7,10,16	4,6,13,15	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	3,7,10,14,18	4,6,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	3,7,10,14,16,17	4,6,13,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	3,7,10,14	4,6,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	3,7,10,14,16,17,18	4,6,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	3,7,10,12	4,6	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	3,7,10,12,16,17,18	4,6,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	3,7,10,12,18	4,6,15,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	3,7,10,12,16,17	4,6,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	3,7,10,12,14,17,18	4,6,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	3,7,10,12,14,16	4,6	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	3,7,10,12,14,17	4,6,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	3,7,10,12,14,16,18	4,6,15,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	3,7,10,12,18	4,6,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	3,7,10,12,16,17	4,6,13,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	3,7,10,12	4,6,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,7,10,12,16,17,18	4,6,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	3,7,10,12,14,17	4,6,13,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	3,7,10,12,14,16,18	4,6,13,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	3,7,10,12,14,17,18	4,6,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	3,7,10,12,14,16	4,6,13,15	$2^{-28.5}$

Table 0.436 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	3,7,10,17	4,6,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	3,7,10,16,18	4,6,11,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	3,7,10,17,18	4,6,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	3,7,10,16	4,6,11,15	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	3,7,10,14,18	4,6,11,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	3,7,10,14,16,17	4,6,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	3,7,10,14	4,6,11,15	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	3,7,10,14,16,17,18	4,6,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	3,7,10,17,18	4,6,11,13,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	3,7,10,16	4,6,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	3,7,10,17	4,6,11,13,15,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	3,7,10,16,18	4,6,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	3,7,10,14	4,6,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	3,7,10,14,16,17,18	4,6,11,13,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	3,7,10,14,18	4,6,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	3,7,10,14,16,17	4,6,11,13,15,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	3,7,10,12,18	4,6,11,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	3,7,10,12,16,17	4,6,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	3,7,10,12	4,6,11,15	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	3,7,10,12,16,17,18	4,6,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	3,7,10,12,14,17	4,6,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	3,7,10,12,14,16,18	4,6,11,18	2^{-34}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	3,7,10,12,14,17,18	4,6,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	3,7,10,12,14,16	4,6,11,15	2^{-34}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	3,7,10,12	4,6,11,13	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	3,7,10,12,16,17,18	4,6,11,13,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	3,7,10,12,18	4,6,11,13,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	3,7,10,12,16,17	4,6,11,13,15,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	3,7,10,12,14,17,18	4,6,11,13,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	3,7,10,12,14,16	4,6,11,13	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	3,7,10,12,14,17	4,6,11,13,15,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	3,7,10,12,14,16,18	4,6,11,13,15,18	$2^{-28.5}$

Table 0.437 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	3,7,18	4,6,9,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	3,7,16,17	4,6,9,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	3,7	4,6,9,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	3,7,16,17,18	4,6,9,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	3,7,14,17	4,6,9,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	3,7,14,16,18	4,6,9,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	3,7,14,17,18	4,6,9,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	3,7,14,16	4,6,9,15	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	3,7	4,6,9,13	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	3,7,16,17,18	4,6,9,13,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	3,7,18	4,6,9,13,15,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	3,7,16,17	4,6,9,13,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	3,7,14,17,18	4,6,9,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	3,7,14,16	4,6,9,13	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	3,7,14,17	4,6,9,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	3,7,14,16,18	4,6,9,13,15,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	3,7,12,17	4,6,9,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	3,7,12,16,18	4,6,9,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	3,7,12,17,18	4,6,9,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	3,7,12,16	4,6,9,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	3,7,12,14,18	4,6,9,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	3,7,12,14,16,17	4,6,9,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	3,7,12,14	4,6,9,15	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	3,7,12,14,16,17,18	4,6,9,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	3,7,12,17,18	4,6,9,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	3,7,12,16	4,6,9,13	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	3,7,12,17	4,6,9,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	3,7,12,16,18	4,6,9,13,15,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	3,7,12,14	4,6,9,13	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	3,7,12,14,16,17,18	4,6,9,13,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	3,7,12,14,18	4,6,9,13,15,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	3,7,12,14,16,17	4,6,9,13,15,17	$2^{-28.5}$

Table 0.438 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	3,7	4,6,9,11	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	3,7,16,17,18	4,6,9,11,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	3,7,18	4,6,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	3,7,16,17	4,6,9,11,15,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	3,7,14,17,18	4,6,9,11,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	3,7,14,16	4,6,9,11	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	3,7,14,17	4,6,9,11,15,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	3,7,14,16,18	4,6,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	3,7,18	4,6,9,11,13,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	3,7,16,17	4,6,9,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	3,7	4,6,9,11,13,15	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	3,7,16,17,18	4,6,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	3,7,14,17	4,6,9,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	3,7,14,16,18	4,6,9,11,13,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	3,7,14,17,18	4,6,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	3,7,14,16	4,6,9,11,13,15	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	3,7,12,17,18	4,6,9,11,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	3,7,12,16	4,6,9,11	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	3,7,12,17	4,6,9,11,15,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	3,7,12,16,18	4,6,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	3,7,12,14	4,6,9,11	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	3,7,12,14,16,17,18	4,6,9,11,17,18	2^{-34}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	3,7,12,14,18	4,6,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	3,7,12,14,16,17	4,6,9,11,15,17	2^{-34}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	3,7,12,17	4,6,9,11,13,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	3,7,12,16,18	4,6,9,11,13,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,7,12,17,18	4,6,9,11,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,7,12,16	4,6,9,11,13,15	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	3,7,12,14,18	4,6,9,11,13,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	3,7,12,14,16,17	4,6,9,11,13,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	3,7,12,14	4,6,9,11,13,15	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	3,7,12,14,16,17,18	4,6,9,11,13,15,17,18	$2^{-28.5}$

Table 0.439 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	3,7,10,17	4,6,9,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	3,7,10,16,18	4,6,9,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	3,7,10,17,18	4,6,9,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	3,7,10,16	4,6,9,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	3,7,10,14,18	4,6,9,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	3,7,10,14,16,17	4,6,9,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	3,7,10,14	4,6,9,15	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	3,7,10,14,16,17,18	4,6,9,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	3,7,10,17,18	4,6,9,13,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	3,7,10,16	4,6,9,13	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	3,7,10,17	4,6,9,13,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	3,7,10,16,18	4,6,9,13,15,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	3,7,10,14	4,6,9,13	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	3,7,10,14,16,17,18	4,6,9,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	3,7,10,14,18	4,6,9,13,15,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	3,7,10,14,16,17	4,6,9,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	3,7,10,12,18	4,6,9,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	3,7,10,12,16,17	4,6,9,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	3,7,10,12	4,6,9,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	3,7,10,12,16,17,18	4,6,9,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	3,7,10,12,14,17	4,6,9,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	3,7,10,12,14,16,18	4,6,9,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	3,7,10,12,14,17,18	4,6,9,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	3,7,10,12,14,16	4,6,9,15	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	3,7,10,12	4,6,9,13	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	3,7,10,12,16,17,18	4,6,9,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	3,7,10,12,18	4,6,9,13,15,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	3,7,10,12,16,17	4,6,9,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	3,7,10,12,14,17,18	4,6,9,13,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	3,7,10,12,14,16	4,6,9,13	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	3,7,10,12,14,17	4,6,9,13,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	3,7,10,12,14,16,18	4,6,9,13,15,18	2^{-23}

Table 0.440 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	3,7,10,17,18	4,6,9,11,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	3,7,10,16	4,6,9,11	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	3,7,10,17	4,6,9,11,15,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,7,10,16,18	4,6,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	3,7,10,14	4,6,9,11	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	3,7,10,14,16,17,18	4,6,9,11,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	3,7,10,14,18	4,6,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	3,7,10,14,16,17	4,6,9,11,15,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	3,7,10,17	4,6,9,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	3,7,10,16,18	4,6,9,11,13,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	3,7,10,17,18	4,6,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	3,7,10,16	4,6,9,11,13,15	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	3,7,10,14,18	4,6,9,11,13,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	3,7,10,14,16,17	4,6,9,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	3,7,10,14	4,6,9,11,13,15	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	3,7,10,14,16,17,18	4,6,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	3,7,10,12	4,6,9,11	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	3,7,10,12,16,17,18	4,6,9,11,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	3,7,10,12,18	4,6,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	3,7,10,12,16,17	4,6,9,11,15,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	3,7,10,12,14,17,18	4,6,9,11,17,18	2^{-1}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	3,7,10,12,14,16	4,6,9,11	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	3,7,10,12,14,17	4,6,9,11,15,17	2^{-1}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	3,7,10,12,14,16,18	4,6,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	3,7,10,12,18	4,6,9,11,13,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	3,7,10,12,16,17	4,6,9,11,13,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	3,7,10,12	4,6,9,11,13,15	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	3,7,10,12,16,17,18	4,6,9,11,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	3,7,10,12,14,17	4,6,9,11,13,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	3,7,10,12,14,16,18	4,6,9,11,13,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	3,7,10,12,14,17,18	4,6,9,11,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	3,7,10,12,14,16	4,6,9,11,13,15	2^{-23}

Table 0.441 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	3,7,17,18	4,6,8,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	3,7,16	4,6,8	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	3,7,17	4,6,8,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	3,7,16,18	4,6,8,15,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	3,7,14	4,6,8	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	3,7,14,16,17,18	4,6,8,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	3,7,14,18	4,6,8,15,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	3,7,14,16,17	4,6,8,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	3,7,17	4,6,8,13,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	3,7,16,18	4,6,8,13,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	3,7,17,18	4,6,8,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	3,7,16	4,6,8,13,15	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	3,7,14,18	4,6,8,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	3,7,14,16,17	4,6,8,13,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	3,7,14	4,6,8,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	3,7,14,16,17,18	4,6,8,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	3,7,12	4,6,8	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	3,7,12,16,17,18	4,6,8,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	3,7,12,18	4,6,8,15,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	3,7,12,16,17	4,6,8,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	3,7,12,14,17,18	4,6,8,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	3,7,12,14,16	4,6,8	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	3,7,12,14,17	4,6,8,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	3,7,12,14,16,18	4,6,8,15,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	3,7,12,18	4,6,8,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	3,7,12,16,17	4,6,8,13,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	3,7,12	4,6,8,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	3,7,12,16,17,18	4,6,8,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	3,7,12,14,17	4,6,8,13,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	3,7,12,14,16,18	4,6,8,13,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	3,7,12,14,17,18	4,6,8,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	3,7,12,14,16	4,6,8,13,15	$2^{-6.5}$

Table 0.442 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	3,7,17	4,6,8,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	3,7,16,18	4,6,8,11,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,7,17,18	4,6,8,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	3,7,16	4,6,8,11,15	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	3,7,14,18	4,6,8,11,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	3,7,14,16,17	4,6,8,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	3,7,14	4,6,8,11,15	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	3,7,14,16,17,18	4,6,8,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	3,7,17,18	4,6,8,11,13,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	3,7,16	4,6,8,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	3,7,17	4,6,8,11,13,15,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	3,7,16,18	4,6,8,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	3,7,14	4,6,8,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	3,7,14,16,17,18	4,6,8,11,13,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	3,7,14,18	4,6,8,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	3,7,14,16,17	4,6,8,11,13,15,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	3,7,12,18	4,6,8,11,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	3,7,12,16,17	4,6,8,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	3,7,12	4,6,8,11,15	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	3,7,12,16,17,18	4,6,8,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	3,7,12,14,17	4,6,8,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	3,7,12,14,16,18	4,6,8,11,18	2^{-1}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	3,7,12,14,17,18	4,6,8,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	3,7,12,14,16	4,6,8,11,15	2^{-1}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	3,7,12	4,6,8,11,13	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	3,7,12,16,17,18	4,6,8,11,13,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	3,7,12,18	4,6,8,11,13,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	3,7,12,16,17	4,6,8,11,13,15,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	3,7,12,14,17,18	4,6,8,11,13,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	3,7,12,14,16	4,6,8,11,13	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	3,7,12,14,17	4,6,8,11,13,15,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	3,7,12,14,16,18	4,6,8,11,13,15,18	$2^{-6.5}$

Table 0.444 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	3,7,10,18	4,6,8,11,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	3,7,10,16,17	4,6,8,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	3,7,10	4,6,8,11,15	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	3,7,10,16,17,18	4,6,8,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	3,7,10,14,17	4,6,8,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	3,7,10,14,16,18	4,6,8,11,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	3,7,10,14,17,18	4,6,8,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	3,7,10,14,16	4,6,8,11,15	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	3,7,10	4,6,8,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	3,7,10,16,17,18	4,6,8,11,13,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	3,7,10,18	4,6,8,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	3,7,10,16,17	4,6,8,11,13,15,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	3,7,10,14,17,18	4,6,8,11,13,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	3,7,10,14,16	4,6,8,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	3,7,10,14,17	4,6,8,11,13,15,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	3,7,10,14,16,18	4,6,8,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	3,7,10,12,17	4,6,8,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	3,7,10,12,16,18	4,6,8,11,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	3,7,10,12,17,18	4,6,8,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,7,10,12,16	4,6,8,11,15	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	3,7,10,12,14,18	4,6,8,11,18	2^{-34}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	3,7,10,12,14,16,17	4,6,8,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	3,7,10,12,14	4,6,8,11,15	2^{-34}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	3,7,10,12,14,16,17,18	4,6,8,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	3,7,10,12,17,18	4,6,8,11,13,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	3,7,10,12,16	4,6,8,11,13	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,7,10,12,17	4,6,8,11,13,15,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,7,10,12,16,18	4,6,8,11,13,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	3,7,10,12,14	4,6,8,11,13	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	3,7,10,12,14,16,17,18	4,6,8,11,13,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	3,7,10,12,14,18	4,6,8,11,13,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	3,7,10,12,14,16,17	4,6,8,11,13,15,17	2^{-12}

Table 0.445 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	3,7,17	4,6,8,9,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	3,7,16,18	4,6,8,9,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	3,7,17,18	4,6,8,9,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	3,7,16	4,6,8,9,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	3,7,14,18	4,6,8,9,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	3,7,14,16,17	4,6,8,9,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	3,7,14	4,6,8,9,15	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	3,7,14,16,17,18	4,6,8,9,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	3,7,17,18	4,6,8,9,13,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	3,7,16	4,6,8,9,13	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	3,7,17	4,6,8,9,13,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	3,7,16,18	4,6,8,9,13,15,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	3,7,14	4,6,8,9,13	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	3,7,14,16,17,18	4,6,8,9,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	3,7,14,18	4,6,8,9,13,15,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	3,7,14,16,17	4,6,8,9,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	3,7,12,18	4,6,8,9,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	3,7,12,16,17	4,6,8,9,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	3,7,12	4,6,8,9,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	3,7,12,16,17,18	4,6,8,9,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	3,7,12,14,17	4,6,8,9,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	3,7,12,14,16,18	4,6,8,9,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	3,7,12,14,17,18	4,6,8,9,15,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	3,7,12,14,16	4,6,8,9,15	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	3,7,12	4,6,8,9,13	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	3,7,12,16,17,18	4,6,8,9,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,7,12,18	4,6,8,9,13,15,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	3,7,12,16,17	4,6,8,9,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	3,7,12,14,17,18	4,6,8,9,13,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	3,7,12,14,16	4,6,8,9,13	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	3,7,12,14,17	4,6,8,9,13,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	3,7,12,14,16,18	4,6,8,9,13,15,18	2^{-12}

Table 0.446 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	3,7,17,18	4,6,8,9,11,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	3,7,16	4,6,8,9,11	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	3,7,17	4,6,8,9,11,15,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	3,7,16,18	4,6,8,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	3,7,14	4,6,8,9,11	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	3,7,14,16,17,18	4,6,8,9,11,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	3,7,14,18	4,6,8,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	3,7,14,16,17	4,6,8,9,11,15,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	3,7,17	4,6,8,9,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	3,7,16,18	4,6,8,9,11,13,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	3,7,17,18	4,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	3,7,16	4,6,8,9,11,13,15	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	3,7,14,18	4,6,8,9,11,13,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	3,7,14,16,17	4,6,8,9,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	3,7,14	4,6,8,9,11,13,15	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	3,7,14,16,17,18	4,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	3,7,12	4,6,8,9,11	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	3,7,12,16,17,18	4,6,8,9,11,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	3,7,12,18	4,6,8,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	3,7,12,16,17	4,6,8,9,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	3,7,12	4,6,8,9,11,13,15	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	3,7,12,16,17,18	4,6,8,9,11,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	3,7,12,14,17	4,6,8,9,11,13,17	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	3,7,12,14,16,18	4,6,8,9,11,13,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	3,7,12,14,17,18	4,6,8,9,11,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	3,7,12,14,16	4,6,8,9,11,13,15	2^{-12}

Table 0.447 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	3,7,10,18	4,6,8,9,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	3,7,10,16,17	4,6,8,9,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	3,7,10	4,6,8,9,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	3,7,10,16,17,18	4,6,8,9,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	3,7,10,14,17	4,6,8,9,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	3,7,10,14,16,18	4,6,8,9,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	3,7,10,14,17,18	4,6,8,9,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	3,7,10,14,16	4,6,8,9,15	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	3,7,10	4,6,8,9,13	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	3,7,10,16,17,18	4,6,8,9,13,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	3,7,10,18	4,6,8,9,13,15,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	3,7,10,16,17	4,6,8,9,13,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	3,7,10,14,17,18	4,6,8,9,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	3,7,10,14,16	4,6,8,9,13	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	3,7,10,14,17	4,6,8,9,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	3,7,10,14,16,18	4,6,8,9,13,15,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	3,7,10,12,17	4,6,8,9,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	3,7,10,12,16,18	4,6,8,9,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	3,7,10,12,17,18	4,6,8,9,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	3,7,10,12,16	4,6,8,9,15	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	3,7,10,12,14,18	4,6,8,9,18	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	3,7,10,12,14,16,17	4,6,8,9,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	3,7,10,12,14	4,6,8,9,15	$2^{-28.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	3,7,10,12,14,16,17,18	4,6,8,9,15,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	3,7,10,12,17,18	4,6,8,9,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	3,7,10,12,16	4,6,8,9,13	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	3,7,10,12,17	4,6,8,9,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,7,10,12,16,18	4,6,8,9,13,15,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	3,7,10,12,14	4,6,8,9,13	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	3,7,10,12,14,16,17,18	4,6,8,9,13,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	3,7,10,12,14,18	4,6,8,9,13,15,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	3,7,10,12,14,16,17	4,6,8,9,13,15,17	$2^{-6.5}$

Table 0.448 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	3,7,10	4,6,8,9,11	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	3,7,10,16,17,18	4,6,8,9,11,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	3,7,10,18	4,6,8,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	3,7,10,16,17	4,6,8,9,11,15,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	3,7,10,14,17,18	4,6,8,9,11,17,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	3,7,10,14,16	4,6,8,9,11	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	3,7,10,14,17	4,6,8,9,11,15,17	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	3,7,10,14,16,18	4,6,8,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	3,7,10,18	4,6,8,9,11,13,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	3,7,10,16,17	4,6,8,9,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	3,7,10	4,6,8,9,11,13,15	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	3,7,10,16,17,18	4,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	3,7,10,14,17	4,6,8,9,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	3,7,10,14,16,18	4,6,8,9,11,13,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	3,7,10,14,17,18	4,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	3,7,10,14,16	4,6,8,9,11,13,15	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	3,7,10,12,17,18	4,6,8,9,11,17,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	3,7,10,12,16	4,6,8,9,11	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	3,7,10,12,17	4,6,8,9,11,15,17	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	3,7,10,12,16,18	4,6,8,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	3,7,10,12,14	4,6,8,9,11	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	3,7,10,12,14,16,17,18	4,6,8,9,11,17,18	2^{-1}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	3,7,10,12,14,18	4,6,8,9,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	3,7,10,12,14,16,17	4,6,8,9,11,15,17	2^{-1}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	3,7,10,12,17	4,6,8,9,11,13,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	3,7,10,12,16,18	4,6,8,9,11,13,18	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	3,7,10,12,17,18	4,6,8,9,11,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	3,7,10,12,16	4,6,8,9,11,13,15	2^{-12}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	3,7,10,12,14,18	4,6,8,9,11,13,18	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	3,7,10,12,14,16,17	4,6,8,9,11,13,17	$2^{-6.5}$
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	3,7,10,12,14	4,6,8,9,11,13,15	2^{-23}
$(0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	3,7,10,12,14,16,17,18	4,6,8,9,11,13,15,17,18	$2^{-6.5}$

Table 0.449 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	3,5,17,18	4,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	3,5,16	4	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	3,5,17	4,15,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	3,5,16,18	4,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	3,5,14	4	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	3,5,14,16,17,18	4,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	3,5,14,18	4,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	3,5,14,16,17	4,15,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	3,5,17	4,13,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	3,5,16,18	4,13,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	3,5,17,18	4,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	3,5,16	4,13,15	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	3,5,14,18	4,13,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	3,5,14,16,17	4,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	3,5,14	4,13,15	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	3,5,14,16,17,18	4,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	3,5,12	4	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	3,5,12,16,17,18	4,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	3,5,12,18	4,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	3,5,12,16,17	4,15,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	3,5,12,14,17,18	4,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	3,5,12,14,16	4	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	3,5,12,14,17	4,15,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	3,5,12,14,16,18	4,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	3,5,12,18	4,13,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	3,5,12,16,17	4,13,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	3,5,12	4,13,15	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	3,5,12,16,17,18	4,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	3,5,12,14,17	4,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	3,5,12,14,16,18	4,13,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	3,5,12,14,17,18	4,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	3,5,12,14,16	4,13,15	2^{-12}

Table 0.450 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	3,5,17	4,11,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	3,5,16,18	4,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	3,5,17,18	4,11,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	3,5,16	4,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	3,5,14,18	4,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	3,5,14,16,17	4,11,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	3,5,14	4,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	3,5,14,16,17,18	4,11,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	3,5,17,18	4,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	3,5,16	4,11,13	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	3,5,17	4,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	3,5,16,18	4,11,13,15,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	3,5,14	4,11,13	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	3,5,14,16,17,18	4,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	3,5,14,18	4,11,13,15,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	3,5,14,16,17	4,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	3,5,12,18	4,11,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	3,5,12,16,17	4,11,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	3,5,12	4,11,15	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	3,5,12,16,17,18	4,11,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	3,5,12,14,17	4,11,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,12,14,16,18	4,11,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	3,5,12,14,17,18	4,11,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,12,14,16	4,11,15	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	3,5,12	4,11,13	2^{-1}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	3,5,12,16,17,18	4,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	3,5,12,18	4,11,13,15,18	2^{-1}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	3,5,12,16,17	4,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	3,5,12,14,17,18	4,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	3,5,12,14,16	4,11,13	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	3,5,12,14,17	4,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	3,5,12,14,16,18	4,11,13,15,18	2^{-12}

Table 0.451 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	3,5,10	4	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	3,5,10,16,17,18	4,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	3,5,10,18	4,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	3,5,10,16,17	4,15,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	3,5,10,14,17,18	4,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	3,5,10,14,16	4	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	3,5,10,14,17	4,15,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	3,5,10,14,16,18	4,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	3,5,10,18	4,13,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,10,16,17	4,13,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	3,5,10	4,13,15	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	3,5,10,16,17,18	4,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	3,5,10,14,17	4,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	3,5,10,14,16,18	4,13,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	3,5,10,14,17,18	4,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	3,5,10,14,16	4,13,15	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	3,5,10,12,17,18	4,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	3,5,10,12,16	4	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	3,5,10,12,17	4,15,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	3,5,10,12,16,18	4,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	3,5,10,12,14	4	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	3,5,10,12,14,16,17,18	4,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	3,5,10,12,14,18	4,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	3,5,10,12,14,16,17	4,15,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,10,12,17	4,13,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	3,5,10,12,16,18	4,13,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,10,12,17,18	4,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	3,5,10,12,16	4,13,15	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	3,5,10,12,14,18	4,13,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	3,5,10,12,14,16,17	4,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	3,5,10,12,14	4,13,15	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	3,5,10,12,14,16,17,18	4,13,15,17,18	$2^{-17.5}$

Table 0.452 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	3,5,10,18	4,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5,10,16,17	4,11,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	3,5,10	4,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5,10,16,17,18	4,11,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,10,14,17	4,11,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	3,5,10,14,16,18	4,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,10,14,17,18	4,11,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	3,5,10,14,16	4,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	3,5,10	4,11,13	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	3,5,10,16,17,18	4,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	3,5,10,18	4,11,13,15,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	3,5,10,16,17	4,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,5,10,14,17,18	4,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,5,10,14,16	4,11,13	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,10,14,17	4,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	3,5,10,14,16,18	4,11,13,15,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	3,5,10,12,17	4,11,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	3,5,10,12,16,18	4,11,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	3,5,10,12,17,18	4,11,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	3,5,10,12,16	4,11,15	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	3,5,10,12,14,18	4,11,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	3,5,10,12,14,16,17	4,11,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	3,5,10,12,14	4,11,15	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	3,5,10,12,14,16,17,18	4,11,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	3,5,10,12,17,18	4,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	3,5,10,12,16	4,11,13	2^{-34}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	3,5,10,12,17	4,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	3,5,10,12,16,18	4,11,13,15,18	2^{-34}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	3,5,10,12,14	4,11,13	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	3,5,10,12,14,16,17,18	4,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	3,5,10,12,14,18	4,11,13,15,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	3,5,10,12,14,16,17	4,11,13,15,17	$2^{-17.5}$

Table 0.453 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	3,5,17	4,9,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	3,5,16,18	4,9,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	3,5,17,18	4,9,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	3,5,16	4,9,15	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	3,5,14,18	4,9,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	3,5,14,16,17	4,9,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	3,5,14	4,9,15	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	3,5,14,16,17,18	4,9,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	3,5,17,18	4,9,13,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	3,5,16	4,9,13	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	3,5,17	4,9,13,15,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	3,5,16,18	4,9,13,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	3,5,14	4,9,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,14,16,17,18	4,9,13,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	3,5,14,18	4,9,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,14,16,17	4,9,13,15,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	3,5,12,18	4,9,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	3,5,12,16,17	4,9,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	3,5,12	4,9,15	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	3,5,12,16,17,18	4,9,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	3,5,12,14,17	4,9,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	3,5,12,14,16,18	4,9,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	3,5,12,14,17,18	4,9,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	3,5,12,14,16	4,9,15	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	3,5,12	4,9,13	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	3,5,12,16,17,18	4,9,13,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	3,5,12,18	4,9,13,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	3,5,12,16,17	4,9,13,15,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	3,5,12,14,17,18	4,9,13,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	3,5,12,14,16	4,9,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	3,5,12,14,17	4,9,13,15,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	3,5,12,14,16,18	4,9,13,15,18	$2^{-17.5}$

Table 0.454 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	3,5,17,18	4,9,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	3,5,16	4,9,11	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	3,5,17	4,9,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	3,5,16,18	4,9,11,15,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	3,5,14	4,9,11	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	3,5,14,16,17,18	4,9,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	3,5,14,18	4,9,11,15,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	3,5,14,16,17	4,9,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	3,5,17	4,9,11,13,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	3,5,16,18	4,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	3,5,17,18	4,9,11,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	3,5,16	4,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	3,5,14,18	4,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	3,5,14,16,17	4,9,11,13,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	3,5,14	4,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	3,5,14,16,17,18	4,9,11,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	3,5,12	4,9,11	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	3,5,12,16,17,18	4,9,11,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	3,5,12,18	4,9,11,15,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	3,5,12,16,17	4,9,11,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	3,5,12,14,17,18	4,9,11,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	3,5,12,14,16	4,9,11	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	3,5,12,14,17	4,9,11,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	3,5,12,14,16,18	4,9,11,15,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	3,5,12,18	4,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	3,5,12,16,17	4,9,11,13,17	2^{-34}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	3,5,12	4,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	3,5,12,16,17,18	4,9,11,13,15,17,18	2^{-34}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	3,5,12,14,17	4,9,11,13,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	3,5,12,14,16,18	4,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	3,5,12,14,17,18	4,9,11,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	3,5,12,14,16	4,9,11,13,15	$2^{-17.5}$

Table 0.455 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	3,5,10,18	4,9,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	3,5,10,16,17	4,9,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	3,5,10	4,9,15	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	3,5,10,16,17,18	4,9,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	3,5,10,14,17	4,9,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	3,5,10,14,16,18	4,9,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	3,5,10,14,17,18	4,9,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	3,5,10,14,16	4,9,15	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	3,5,10	4,9,13	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	3,5,10,16,17,18	4,9,13,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	3,5,10,18	4,9,13,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	3,5,10,16,17	4,9,13,15,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,10,14,17,18	4,9,13,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	3,5,10,14,16	4,9,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,10,14,17	4,9,13,15,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	3,5,10,14,16,18	4,9,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	3,5,10,12,17	4,9,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	3,5,10,12,16,18	4,9,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	3,5,10,12,17,18	4,9,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	3,5,10,12,16	4,9,15	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	3,5,10,12,14,18	4,9,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	3,5,10,12,14,16,17	4,9,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,10,12,14	4,9,15	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	3,5,10,12,14,16,17,18	4,9,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	3,5,10,12,17,18	4,9,13,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	3,5,10,12,16	4,9,13	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	3,5,10,12,17	4,9,13,15,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	3,5,10,12,16,18	4,9,13,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	3,5,10,12,14	4,9,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	3,5,10,12,14,16,17,18	4,9,13,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	3,5,10,12,14,18	4,9,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	3,5,10,12,14,16,17	4,9,13,15,17	2^{-12}

Table 0.456 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	3,5,10	4,9,11	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	3,5,10,16,17,18	4,9,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	3,5,10,18	4,9,11,15,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	3,5,10,16,17	4,9,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	3,5,10,14,17,18	4,9,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	3,5,10,14,16	4,9,11	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	3,5,10,14,17	4,9,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	3,5,10,14,16,18	4,9,11,15,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	3,5,10,18	4,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	3,5,10,16,17	4,9,11,13,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	3,5,10	4,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	3,5,10,16,17,18	4,9,11,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	3,5,10,14,17	4,9,11,13,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	3,5,10,14,16,18	4,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	3,5,10,14,17,18	4,9,11,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	3,5,10,14,16	4,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	3,5,10,12,17,18	4,9,11,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	3,5,10,12,16	4,9,11	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	3,5,10,12,17	4,9,11,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	3,5,10,12,16,18	4,9,11,15,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	3,5,10,12,14	4,9,11	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	3,5,10,12,14,16,17,18	4,9,11,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	3,5,10,12,14,18	4,9,11,15,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	3,5,10,12,14,16,17	4,9,11,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	3,5,10,12,17	4,9,11,13,17	2^{-1}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	3,5,10,12,16,18	4,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	3,5,10,12,17,18	4,9,11,13,15,17,18	2^{-1}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	3,5,10,12,16	4,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	3,5,10,12,14,18	4,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	3,5,10,12,14,16,17	4,9,11,13,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	3,5,10,12,14	4,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	3,5,10,12,14,16,17,18	4,9,11,13,15,17,18	2^{-12}

Table 0.457 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	3,5	4,8	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	3,5,16,17,18	4,8,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	3,5,18	4,8,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	3,5,16,17	4,8,15,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	3,5,14,17,18	4,8,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	3,5,14,16	4,8	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	3,5,14,17	4,8,15,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	3,5,14,16,18	4,8,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	3,5,18	4,8,13,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	3,5,16,17	4,8,13,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	3,5	4,8,13,15	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	3,5,16,17,18	4,8,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	3,5,14,17	4,8,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,14,16,18	4,8,13,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	3,5,14,17,18	4,8,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,14,16	4,8,13,15	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	3,5,12,17,18	4,8,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	3,5,12,16	4,8	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	3,5,12,17	4,8,15,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	3,5,12,16,18	4,8,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	3,5,12,14	4,8	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	3,5,12,14,16,17,18	4,8,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	3,5,12,14,18	4,8,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,12,14,16,17	4,8,15,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	3,5,12,17	4,8,13,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	3,5,12,16,18	4,8,13,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	3,5,12,17,18	4,8,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	3,5,12,16	4,8,13,15	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	3,5,12,14,18	4,8,13,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	3,5,12,14,16,17	4,8,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	3,5,12,14	4,8,13,15	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	3,5,12,14,16,17,18	4,8,13,15,17,18	$2^{-17.5}$

Table 0.458 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	3,5,18	4,8,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	3,5,16,17	4,8,11,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	3,5	4,8,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	3,5,16,17,18	4,8,11,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	3,5,14,17	4,8,11,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	3,5,14,16,18	4,8,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	3,5,14,17,18	4,8,11,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	3,5,14,16	4,8,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	3,5	4,8,11,13	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	3,5,16,17,18	4,8,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	3,5,18	4,8,11,13,15,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	3,5,16,17	4,8,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	3,5,14,17,18	4,8,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	3,5,14,16	4,8,11,13	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	3,5,14,17	4,8,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	3,5,14,16,18	4,8,11,13,15,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	3,5,12,17	4,8,11,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	3,5,12,16,18	4,8,11,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	3,5,12,17,18	4,8,11,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	3,5,12,16	4,8,11,15	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	3,5,12,14,18	4,8,11,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	3,5,12,14,16,17	4,8,11,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	3,5,12,14	4,8,11,15	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	3,5,12,14,16,17,18	4,8,11,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	3,5,12,17,18	4,8,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	3,5,12,16	4,8,11,13	2^{-1}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	3,5,12,17	4,8,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	3,5,12,16,18	4,8,11,13,15,18	2^{-1}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	3,5,12,14	4,8,11,13	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	3,5,12,14,16,17,18	4,8,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	3,5,12,14,18	4,8,11,13,15,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	3,5,12,14,16,17	4,8,11,13,15,17	$2^{-17.5}$

Table 0.459 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	3,5,10,17,18	4,8,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	3,5,10,16	4,8	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	3,5,10,17	4,8,15,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	3,5,10,16,18	4,8,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	3,5,10,14	4,8	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	3,5,10,14,16,17,18	4,8,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	3,5,10,14,18	4,8,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	3,5,10,14,16,17	4,8,15,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	3,5,10,17	4,8,13,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	3,5,10,16,18	4,8,13,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	3,5,10,17,18	4,8,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	3,5,10,16	4,8,13,15	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,10,14,18	4,8,13,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	3,5,10,14,16,17	4,8,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,10,14	4,8,13,15	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	3,5,10,14,16,17,18	4,8,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	3,5,10,12	4,8	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	3,5,10,12,16,17,18	4,8,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	3,5,10,12,18	4,8,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	3,5,10,12,16,17	4,8,15,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	3,5,10,12,14,17,18	4,8,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	3,5,10,12,14,16	4,8	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	3,5,10,12,14,17	4,8,15,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	3,5,10,12,14,16,18	4,8,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	3,5,10,12,18	4,8,13,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	3,5,10,12,16,17	4,8,13,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	3,5,10,12	4,8,13,15	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	3,5,10,12,16,17,18	4,8,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	3,5,10,12,14,17	4,8,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	3,5,10,12,14,16,18	4,8,13,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	3,5,10,12,14,17,18	4,8,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	3,5,10,12,14,16	4,8,13,15	2^{-23}

Table 0.460 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	3,5,10,17	4,8,11,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	3,5,10,16,18	4,8,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	3,5,10,17,18	4,8,11,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	3,5,10,16	4,8,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	3,5,10,14,18	4,8,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	3,5,10,14,16,17	4,8,11,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	3,5,10,14	4,8,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	3,5,10,14,16,17,18	4,8,11,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	3,5,10,17,18	4,8,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	3,5,10,16	4,8,11,13	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	3,5,10,17	4,8,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	3,5,10,16,18	4,8,11,13,15,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	3,5,10,14	4,8,11,13	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	3,5,10,14,16,17,18	4,8,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	3,5,10,14,18	4,8,11,13,15,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	3,5,10,14,16,17	4,8,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	3,5,10,12,18	4,8,11,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	3,5,10,12,16,17	4,8,11,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	3,5,10,12	4,8,11,15	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	3,5,10,12,16,17,18	4,8,11,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	3,5,10,12,14,17	4,8,11,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	3,5,10,12,14,16,18	4,8,11,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	3,5,10,12,14,17,18	4,8,11,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	3,5,10,12,14,16	4,8,11,15	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	3,5,10,12	4,8,11,13	2^{-34}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	3,5,10,12,16,17,18	4,8,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	3,5,10,12,18	4,8,11,13,15,18	2^{-34}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	3,5,10,12,16,17	4,8,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	3,5,10,12,14,17,18	4,8,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	3,5,10,12,14,16	4,8,11,13	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	3,5,10,12,14,17	4,8,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	3,5,10,12,14,16,18	4,8,11,13,15,18	2^{-23}

Table 0.461 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	3,5,18	4,8,9,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	3,5,16,17	4,8,9,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	3,5	4,8,9,15	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	3,5,16,17,18	4,8,9,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	3,5,14,17	4,8,9,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	3,5,14,16,18	4,8,9,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	3,5,14,17,18	4,8,9,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	3,5,14,16	4,8,9,15	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	3,5	4,8,9,13	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	3,5,16,17,18	4,8,9,13,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	3,5,18	4,8,9,13,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	3,5,16,17	4,8,9,13,15,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	3,5,14,17,18	4,8,9,13,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	3,5,14,16	4,8,9,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	3,5,14,17	4,8,9,13,15,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	3,5,14,16,18	4,8,9,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	3,5,12,17	4,8,9,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	3,5,12,16,18	4,8,9,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	3,5,12,17,18	4,8,9,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	3,5,12,16	4,8,9,15	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	3,5,12,14,18	4,8,9,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	3,5,12,14,16,17	4,8,9,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	3,5,12,14	4,8,9,15	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	3,5,12,14,16,17,18	4,8,9,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	3,5,12,17,18	4,8,9,13,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,12,16	4,8,9,13	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	3,5,12,17	4,8,9,13,15,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,12,16,18	4,8,9,13,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	3,5,12,14	4,8,9,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	3,5,12,14,16,17,18	4,8,9,13,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	3,5,12,14,18	4,8,9,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	3,5,12,14,16,17	4,8,9,13,15,17	2^{-23}

Table 0.462 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5	4,8,9,11	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	3,5,16,17,18	4,8,9,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5,18	4,8,9,11,15,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	3,5,16,17	4,8,9,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	3,5,14,17,18	4,8,9,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,14,16	4,8,9,11	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	3,5,14,17	4,8,9,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,14,16,18	4,8,9,11,15,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	3,5,18	4,8,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	3,5,16,17	4,8,9,11,13,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	3,5	4,8,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	3,5,16,17,18	4,8,9,11,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,5,14,17	4,8,9,11,13,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,5,14,16,18	4,8,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	3,5,14,17,18	4,8,9,11,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	3,5,14,16	4,8,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	3,5,12,17,18	4,8,9,11,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	3,5,12,16	4,8,9,11	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	3,5,12,17	4,8,9,11,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	3,5,12,16,18	4,8,9,11,15,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	3,5,12,14	4,8,9,11	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	3,5,12,14,16,17,18	4,8,9,11,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	3,5,12,14,18	4,8,9,11,15,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	3,5,12,14,16,17	4,8,9,11,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	3,5,12,17	4,8,9,11,13,17	2^{-34}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	3,5,12,16,18	4,8,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	3,5,12,17,18	4,8,9,11,13,15,17,18	2^{-34}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	3,5,12,16	4,8,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	3,5,12,14,18	4,8,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	3,5,12,14,16,17	4,8,9,11,13,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	3,5,12,14	4,8,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	3,5,12,14,16,17,18	4,8,9,11,13,15,17,18	2^{-23}

Table 0.463 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	3,5,10,17	4,8,9,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	3,5,10,16,18	4,8,9,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	3,5,10,17,18	4,8,9,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	3,5,10,16	4,8,9,15	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	3,5,10,14,18	4,8,9,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	3,5,10,14,16,17	4,8,9,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	3,5,10,14	4,8,9,15	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	3,5,10,14,16,17,18	4,8,9,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	3,5,10,17,18	4,8,9,13,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	3,5,10,16	4,8,9,13	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	3,5,10,17	4,8,9,13,15,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	3,5,10,16,18	4,8,9,13,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	3,5,10,14	4,8,9,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	3,5,10,14,16,17,18	4,8,9,13,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	3,5,10,14,18	4,8,9,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	3,5,10,14,16,17	4,8,9,13,15,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	3,5,10,12,18	4,8,9,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	3,5,10,12,16,17	4,8,9,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	3,5,10,12	4,8,9,15	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	3,5,10,12,16,17,18	4,8,9,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	3,5,10,12,14,17	4,8,9,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	3,5,10,12,14,16,18	4,8,9,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	3,5,10,12,14,17,18	4,8,9,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	3,5,10,12,14,16	4,8,9,15	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	3,5,10,12	4,8,9,13	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	3,5,10,12,16,17,18	4,8,9,13,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	3,5,10,12,18	4,8,9,13,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	3,5,10,12,16,17	4,8,9,13,15,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	3,5,10,12,14,17,18	4,8,9,13,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	3,5,10,12,14,16	4,8,9,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	3,5,10,12,14,17	4,8,9,13,15,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	3,5,10,12,14,16,18	4,8,9,13,15,18	$2^{-17.5}$

Table 0.464 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	3,5,10,17,18	4,8,9,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	3,5,10,16	4,8,9,11	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	3,5,10,17	4,8,9,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	3,5,10,16,18	4,8,9,11,15,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	3,5,10,14	4,8,9,11	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	3,5,10,14,16,17,18	4,8,9,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	3,5,10,14,18	4,8,9,11,15,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	3,5,10,14,16,17	4,8,9,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	3,5,10,17	4,8,9,11,13,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	3,5,10,16,18	4,8,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	3,5,10,17,18	4,8,9,11,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	3,5,10,16	4,8,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	3,5,10,14,18	4,8,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	3,5,10,14,16,17	4,8,9,11,13,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	3,5,10,14	4,8,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	3,5,10,14,16,17,18	4,8,9,11,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	3,5,10,12	4,8,9,11	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	3,5,10,12,16,17,18	4,8,9,11,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	3,5,10,12,18	4,8,9,11,15,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	3,5,10,12,16,17	4,8,9,11,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,10,12,14,17,18	4,8,9,11,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	3,5,10,12,14,16	4,8,9,11	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,10,12,14,17	4,8,9,11,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	3,5,10,12,14,16,18	4,8,9,11,15,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	3,5,10,12,18	4,8,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	3,5,10,12,16,17	4,8,9,11,13,17	2^{-1}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	3,5,10,12	4,8,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	3,5,10,12,16,17,18	4,8,9,11,13,15,17,18	2^{-1}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	3,5,10,12,14,17	4,8,9,11,13,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	3,5,10,12,14,16,18	4,8,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	3,5,10,12,14,17,18	4,8,9,11,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	3,5,10,12,14,16	4,8,9,11,13,15	$2^{-17.5}$

Table 0.465 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	3,5,7,17	4,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	3,5,7,16,18	4,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	3,5,7,17,18	4,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	3,5,7,16	4,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	3,5,7,14,18	4,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	3,5,7,14,16,17	4,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	3,5,7,14	4,15	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	3,5,7,14,16,17,18	4,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,7,17,18	4,13,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	3,5,7,16	4,13	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	3,5,7,17	4,13,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	3,5,7,16,18	4,13,15,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	3,5,7,14	4,13	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	3,5,7,14,16,17,18	4,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	3,5,7,14,18	4,13,15,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	3,5,7,14,16,17	4,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	3,5,7,12,18	4,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	3,5,7,12,16,17	4,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	3,5,7,12	4,15	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	3,5,7,12,16,17,18	4,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	3,5,7,12,14,17	4,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	3,5,7,12,14,16,18	4,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	3,5,7,12,14,17,18	4,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	3,5,7,12,14,16	4,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	3,5,7,12	4,13	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	3,5,7,12,16,17,18	4,13,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	3,5,7,12,18	4,13,15,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	3,5,7,12,16,17	4,13,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	3,5,7,12,14,17,18	4,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	3,5,7,12,14,16	4,13	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	3,5,7,12,14,17	4,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	3,5,7,12,14,16,18	4,13,15,18	2^{-12}

Table 0.466 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	3,5,7,17,18	4,11,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	3,5,7,16	4,11	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	3,5,7,17	4,11,15,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	3,5,7,16,18	4,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	3,5,7,14	4,11	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	3,5,7,14,16,17,18	4,11,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	3,5,7,14,18	4,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	3,5,7,14,16,17	4,11,15,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	3,5,7,17	4,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,7,16,18	4,11,13,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	3,5,7,17,18	4,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	3,5,7,16	4,11,13,15	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	3,5,7,14,18	4,11,13,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,7,14,16,17	4,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	3,5,7,14	4,11,13,15	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,7,14,16,17,18	4,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	3,5,7,12	4,11	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	3,5,7,12,16,17,18	4,11,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	3,5,7,12,18	4,11,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	3,5,7,12,16,17	4,11,15,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	3,5,7,12,14,17,18	4,11,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	3,5,7,12,14,16	4,11	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	3,5,7,12,14,17	4,11,15,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	3,5,7,12,14,16,18	4,11,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	3,5,7,12,18	4,11,13,18	2^{-1}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	3,5,7,12,16,17	4,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	3,5,7,12	4,11,13,15	2^{-1}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	3,5,7,12,16,17,18	4,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	3,5,7,12,14,17	4,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	3,5,7,12,14,16,18	4,11,13,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	3,5,7,12,14,17,18	4,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	3,5,7,12,14,16	4,11,13,15	2^{-12}

Table 0.467 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	3,5,7,10,18	4,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	3,5,7,10,16,17	4,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	3,5,7,10	4,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	3,5,7,10,16,17,18	4,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	3,5,7,10,14,17	4,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	3,5,7,10,14,16,18	4,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	3,5,7,10,14,17,18	4,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	3,5,7,10,14,16	4,15	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	3,5,7,10	4,13	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	3,5,7,10,16,17,18	4,13,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	3,5,7,10,18	4,13,15,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	3,5,7,10,16,17	4,13,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	3,5,7,10,14,17,18	4,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	3,5,7,10,14,16	4,13	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	3,5,7,10,14,17	4,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	3,5,7,10,14,16,18	4,13,15,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	3,5,7,10,12,17	4,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	3,5,7,10,12,16,18	4,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	3,5,7,10,12,17,18	4,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	3,5,7,10,12,16	4,15	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	3,5,7,10,12,14,18	4,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	3,5,7,10,12,14,16,17	4,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	3,5,7,10,12,14	4,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	3,5,7,10,12,14,16,17,18	4,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	3,5,7,10,12,17,18	4,13,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	3,5,7,10,12,16	4,13	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	3,5,7,10,12,17	4,13,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	3,5,7,10,12,16,18	4,13,15,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	3,5,7,10,12,14	4,13	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	3,5,7,10,12,14,16,17,18	4,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	3,5,7,10,12,14,18	4,13,15,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	3,5,7,10,12,14,16,17	4,13,15,17	$2^{-17.5}$

Table 0.468 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	3,5,7,10	4,11	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	3,5,7,10,16,17,18	4,11,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	3,5,7,10,18	4,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	3,5,7,10,16,17	4,11,15,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	3,5,7,10,14,17,18	4,11,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	3,5,7,10,14,16	4,11	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	3,5,7,10,14,17	4,11,15,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	3,5,7,10,14,16,18	4,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	3,5,7,10,18	4,11,13,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	3,5,7,10,16,17	4,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	3,5,7,10	4,11,13,15	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	3,5,7,10,16,17,18	4,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,7,10,14,17	4,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	3,5,7,10,14,16,18	4,11,13,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,7,10,14,17,18	4,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	3,5,7,10,14,16	4,11,13,15	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	3,5,7,10,12,17,18	4,11,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	3,5,7,10,12,16	4,11	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	3,5,7,10,12,17	4,11,15,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	3,5,7,10,12,16,18	4,11,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	3,5,7,10,12,14	4,11	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,5,7,10,12,14,16,17,18	4,11,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	3,5,7,10,12,14,18	4,11,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	3,5,7,10,12,14,16,17	4,11,15,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	3,5,7,10,12,17	4,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	3,5,7,10,12,16,18	4,11,13,18	2^{-34}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	3,5,7,10,12,17,18	4,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	3,5,7,10,12,16	4,11,13,15	2^{-34}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	3,5,7,10,12,14,18	4,11,13,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	3,5,7,10,12,14,16,17	4,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	3,5,7,10,12,14	4,11,13,15	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	3,5,7,10,12,14,16,17,18	4,11,13,15,17,18	$2^{-17.5}$

Table 0.469 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	3,5,7,17,18	4,9,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	3,5,7,16	4,9	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	3,5,7,17	4,9,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	3,5,7,16,18	4,9,15,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	3,5,7,14	4,9	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	3,5,7,14,16,17,18	4,9,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	3,5,7,14,18	4,9,15,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	3,5,7,14,16,17	4,9,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	3,5,7,17	4,9,13,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	3,5,7,16,18	4,9,13,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	3,5,7,17,18	4,9,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	3,5,7,16	4,9,13,15	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	3,5,7,14,18	4,9,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	3,5,7,14,16,17	4,9,13,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	3,5,7,14	4,9,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	3,5,7,14,16,17,18	4,9,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,12	4,9	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	3,5,7,12,16,17,18	4,9,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,12,18	4,9,15,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	3,5,7,12,16,17	4,9,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	3,5,7,12,14,17,18	4,9,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,12,14,16	4,9	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	3,5,7,12,14,17	4,9,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,12,14,16,18	4,9,15,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	3,5,7,12,18	4,9,13,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	3,5,7,12,16,17	4,9,13,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	3,5,7,12	4,9,13,15	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	3,5,7,12,16,17,18	4,9,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	3,5,7,12,14,17	4,9,13,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	3,5,7,12,14,16,18	4,9,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	3,5,7,12,14,17,18	4,9,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	3,5,7,12,14,16	4,9,13,15	$2^{-17.5}$

Table 0.470 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	3,5,7,17	4,9,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	3,5,7,16,18	4,9,11,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	3,5,7,17,18	4,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	3,5,7,16	4,9,11,15	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	3,5,7,14,18	4,9,11,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	3,5,7,14,16,17	4,9,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	3,5,7,14	4,9,11,15	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	3,5,7,14,16,17,18	4,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	3,5,7,17,18	4,9,11,13,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	3,5,7,16	4,9,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	3,5,7,17	4,9,11,13,15,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	3,5,7,16,18	4,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	3,5,7,14	4,9,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,5,7,14,16,17,18	4,9,11,13,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	3,5,7,14,18	4,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	3,5,7,14,16,17	4,9,11,13,15,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	3,5,7,12,18	4,9,11,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	3,5,7,12,16,17	4,9,11,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	3,5,7,12	4,9,11,15	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	3,5,7,12,16,17,18	4,9,11,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	3,5,7,12,14,17	4,9,11,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	3,5,7,12,14,16,18	4,9,11,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	3,5,7,12,14,17,18	4,9,11,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	3,5,7,12,14,16	4,9,11,15	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	3,5,7,12	4,9,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	3,5,7,12,16,17,18	4,9,11,13,17,18	2^{-34}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	3,5,7,12,18	4,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	3,5,7,12,16,17	4,9,11,13,15,17	2^{-34}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	3,5,7,12,14,17,18	4,9,11,13,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	3,5,7,12,14,16	4,9,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	3,5,7,12,14,17	4,9,11,13,15,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	3,5,7,12,14,16,18	4,9,11,13,15,18	$2^{-17.5}$

Table 0.471 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	3,5,7,10	4,9	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5,7,10,16,17,18	4,9,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	3,5,7,10,18	4,9,15,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5,7,10,16,17	4,9,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,10,14,17,18	4,9,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	3,5,7,10,14,16	4,9	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,10,14,17	4,9,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	3,5,7,10,14,16,18	4,9,15,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	3,5,7,10,18	4,9,13,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	3,5,7,10,16,17	4,9,13,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	3,5,7,10	4,9,13,15	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	3,5,7,10,16,17,18	4,9,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	3,5,7,10,14,17	4,9,13,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	3,5,7,10,14,16,18	4,9,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,5,7,10,14,17,18	4,9,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,5,7,10,14,16	4,9,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	3,5,7,10,12,17,18	4,9,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	3,5,7,10,12,16	4,9	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	3,5,7,10,12,17	4,9,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	3,5,7,10,12,16,18	4,9,15,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	3,5,7,10,12,14	4,9	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	3,5,7,10,12,14,16,17,18	4,9,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	3,5,7,10,12,14,18	4,9,15,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	3,5,7,10,12,14,16,17	4,9,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	3,5,7,10,12,17	4,9,13,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	3,5,7,10,12,16,18	4,9,13,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	3,5,7,10,12,17,18	4,9,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	3,5,7,10,12,16	4,9,13,15	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	3,5,7,10,12,14,18	4,9,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	3,5,7,10,12,14,16,17	4,9,13,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	3,5,7,10,12,14	4,9,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	3,5,7,10,12,14,16,17,18	4,9,13,15,17,18	2^{-12}

Table 0.472 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	3,5,7,10,18	4,9,11,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	3,5,7,10,16,17	4,9,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	3,5,7,10	4,9,11,15	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	3,5,7,10,16,17,18	4,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	3,5,7,10,14,17	4,9,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	3,5,7,10,14,16,18	4,9,11,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	3,5,7,10,14,17,18	4,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	3,5,7,10,14,16	4,9,11,15	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	3,5,7,10	4,9,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	3,5,7,10,16,17,18	4,9,11,13,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	3,5,7,10,18	4,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	3,5,7,10,16,17	4,9,11,13,15,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	3,5,7,10,14,17,18	4,9,11,13,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	3,5,7,10,14,16	4,9,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	3,5,7,10,14,17	4,9,11,13,15,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	3,5,7,10,14,16,18	4,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	3,5,7,10,12,17	4,9,11,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	3,5,7,10,12,16,18	4,9,11,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	3,5,7,10,12,17,18	4,9,11,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	3,5,7,10,12,16	4,9,11,15	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	3,5,7,10,12,14,18	4,9,11,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	3,5,7,10,12,14,16,17	4,9,11,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	3,5,7,10,12,14	4,9,11,15	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	3,5,7,10,12,14,16,17,18	4,9,11,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,7,10,12,17,18	4,9,11,13,17,18	2^{-1}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	3,5,7,10,12,16	4,9,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,7,10,12,17	4,9,11,13,15,17	2^{-1}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	3,5,7,10,12,16,18	4,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	3,5,7,10,12,14	4,9,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	3,5,7,10,12,14,16,17,18	4,9,11,13,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	3,5,7,10,12,14,18	4,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	3,5,7,10,12,14,16,17	4,9,11,13,15,17	2^{-12}

Table 0.473 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5,7,18	4,8,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	3,5,7,16,17	4,8,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5,7	4,8,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	3,5,7,16,17,18	4,8,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	3,5,7,14,17	4,8,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,14,16,18	4,8,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	3,5,7,14,17,18	4,8,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,14,16	4,8,15	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	3,5,7	4,8,13	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	3,5,7,16,17,18	4,8,13,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	3,5,7,18	4,8,13,15,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	3,5,7,16,17	4,8,13,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	3,5,7,14,17,18	4,8,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	3,5,7,14,16	4,8,13	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,5,7,14,17	4,8,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,5,7,14,16,18	4,8,13,15,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	3,5,7,12,17	4,8,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	3,5,7,12,16,18	4,8,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	3,5,7,12,17,18	4,8,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	3,5,7,12,16	4,8,15	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	3,5,7,12,14,18	4,8,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	3,5,7,12,14,16,17	4,8,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	3,5,7,12,14	4,8,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	3,5,7,12,14,16,17,18	4,8,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	3,5,7,12,17,18	4,8,13,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	3,5,7,12,16	4,8,13	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	3,5,7,12,17	4,8,13,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	3,5,7,12,16,18	4,8,13,15,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	3,5,7,12,14	4,8,13	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	3,5,7,12,14,16,17,18	4,8,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	3,5,7,12,14,18	4,8,13,15,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	3,5,7,12,14,16,17	4,8,13,15,17	$2^{-17.5}$

Table 0.474 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	3,5,7	4,8,11	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	3,5,7,16,17,18	4,8,11,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	3,5,7,18	4,8,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	3,5,7,16,17	4,8,11,15,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	3,5,7,14,17,18	4,8,11,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	3,5,7,14,16	4,8,11	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	3,5,7,14,17	4,8,11,15,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	3,5,7,14,16,18	4,8,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	3,5,7,18	4,8,11,13,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	3,5,7,16,17	4,8,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	3,5,7	4,8,11,13,15	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	3,5,7,16,17,18	4,8,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	3,5,7,14,17	4,8,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	3,5,7,14,16,18	4,8,11,13,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	3,5,7,14,17,18	4,8,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	3,5,7,14,16	4,8,11,13,15	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	3,5,7,12,17,18	4,8,11,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	3,5,7,12,16	4,8,11	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	3,5,7,12,17	4,8,11,15,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	3,5,7,12,16,18	4,8,11,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	3,5,7,12,14	4,8,11	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	3,5,7,12,14,16,17,18	4,8,11,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	3,5,7,12,14,18	4,8,11,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	3,5,7,12,14,16,17	4,8,11,15,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	3,5,7,12,17	4,8,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,7,12,16,18	4,8,11,13,18	2^{-1}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	3,5,7,12,17,18	4,8,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,7,12,16	4,8,11,13,15	2^{-1}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	3,5,7,12,14,18	4,8,11,13,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	3,5,7,12,14,16,17	4,8,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	3,5,7,12,14	4,8,11,13,15	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	3,5,7,12,14,16,17,18	4,8,11,13,15,17,18	$2^{-17.5}$

Table 0.475 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	3,5,7,10,17	4,8,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	3,5,7,10,16,18	4,8,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	3,5,7,10,17,18	4,8,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	3,5,7,10,16	4,8,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	3,5,7,10,14,18	4,8,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	3,5,7,10,14,16,17	4,8,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	3,5,7,10,14	4,8,15	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	3,5,7,10,14,16,17,18	4,8,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	3,5,7,10,17,18	4,8,13,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	3,5,7,10,16	4,8,13	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	3,5,7,10,17	4,8,13,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	3,5,7,10,16,18	4,8,13,15,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	3,5,7,10,14	4,8,13	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	3,5,7,10,14,16,17,18	4,8,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	3,5,7,10,14,18	4,8,13,15,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	3,5,7,10,14,16,17	4,8,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	3,5,7,10,12,18	4,8,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,10,12,16,17	4,8,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	3,5,7,10,12	4,8,15	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,10,12,16,17,18	4,8,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,10,12,14,17	4,8,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	3,5,7,10,12,14,16,18	4,8,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,10,12,14,17,18	4,8,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	3,5,7,10,12,14,16	4,8,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	3,5,7,10,12	4,8,13	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	3,5,7,10,12,16,17,18	4,8,13,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	3,5,7,10,12,18	4,8,13,15,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	3,5,7,10,12,16,17	4,8,13,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	3,5,7,10,12,14,17,18	4,8,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	3,5,7,10,12,14,16	4,8,13	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	3,5,7,10,12,14,17	4,8,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	3,5,7,10,12,14,16,18	4,8,13,15,18	2^{-23}

Table 0.476 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	3,5,7,10,17,18	4,8,11,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	3,5,7,10,16	4,8,11	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	3,5,7,10,17	4,8,11,15,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	3,5,7,10,16,18	4,8,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	3,5,7,10,14	4,8,11	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	3,5,7,10,14,16,17,18	4,8,11,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	3,5,7,10,14,18	4,8,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	3,5,7,10,14,16,17	4,8,11,15,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	3,5,7,10,17	4,8,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	3,5,7,10,16,18	4,8,11,13,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	3,5,7,10,17,18	4,8,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	3,5,7,10,16	4,8,11,13,15	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	3,5,7,10,14,18	4,8,11,13,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	3,5,7,10,14,16,17	4,8,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	3,5,7,10,14	4,8,11,13,15	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	3,5,7,10,14,16,17,18	4,8,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	3,5,7,10,12	4,8,11	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	3,5,7,10,12,16,17,18	4,8,11,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	3,5,7,10,12,18	4,8,11,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	3,5,7,10,12,16,17	4,8,11,15,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	3,5,7,10,12,14,17,18	4,8,11,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	3,5,7,10,12,14,16	4,8,11	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	3,5,7,10,12,14,17	4,8,11,15,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	3,5,7,10,12,14,16,18	4,8,11,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	3,5,7,10,12,18	4,8,11,13,18	2^{-34}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	3,5,7,10,12,16,17	4,8,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	3,5,7,10,12	4,8,11,13,15	2^{-34}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	3,5,7,10,12,16,17,18	4,8,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	3,5,7,10,12,14,17	4,8,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	3,5,7,10,12,14,16,18	4,8,11,13,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	3,5,7,10,12,14,17,18	4,8,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	3,5,7,10,12,14,16	4,8,11,13,15	2^{-23}

Table 0.477 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	3,5,7	4,8,9	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	3,5,7,16,17,18	4,8,9,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	3,5,7,18	4,8,9,15,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	3,5,7,16,17	4,8,9,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	3,5,7,14,17,18	4,8,9,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	3,5,7,14,16	4,8,9	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	3,5,7,14,17	4,8,9,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	3,5,7,14,16,18	4,8,9,15,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	3,5,7,18	4,8,9,13,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	3,5,7,16,17	4,8,9,13,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	3,5,7	4,8,9,13,15	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	3,5,7,16,17,18	4,8,9,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	3,5,7,14,17	4,8,9,13,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	3,5,7,14,16,18	4,8,9,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	3,5,7,14,17,18	4,8,9,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	3,5,7,14,16	4,8,9,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	3,5,7,12,17,18	4,8,9,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	3,5,7,12,16	4,8,9	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	3,5,7,12,17	4,8,9,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	3,5,7,12,16,18	4,8,9,15,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	3,5,7,12,14	4,8,9	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	3,5,7,12,14,16,17,18	4,8,9,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	3,5,7,12,14,18	4,8,9,15,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	3,5,7,12,14,16,17	4,8,9,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	3,5,7,12,17	4,8,9,13,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	3,5,7,12,16,18	4,8,9,13,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	3,5,7,12,17,18	4,8,9,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	3,5,7,12,16	4,8,9,13,15	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	3,5,7,12,14,18	4,8,9,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	3,5,7,12,14,16,17	4,8,9,13,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	3,5,7,12,14	4,8,9,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	3,5,7,12,14,16,17,18	4,8,9,13,15,17,18	2^{-23}

Table 0.478 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	3,5,7,18	4,8,9,11,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	3,5,7,16,17	4,8,9,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	3,5,7	4,8,9,11,15	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	3,5,7,16,17,18	4,8,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	3,5,7,14,17	4,8,9,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	3,5,7,14,16,18	4,8,9,11,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	3,5,7,14,17,18	4,8,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	3,5,7,14,16	4,8,9,11,15	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	3,5,7	4,8,9,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	3,5,7,16,17,18	4,8,9,11,13,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	3,5,7,18	4,8,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	3,5,7,16,17	4,8,9,11,13,15,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	3,5,7,14,17,18	4,8,9,11,13,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,7,14,16	4,8,9,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	3,5,7,14,17	4,8,9,11,13,15,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,7,14,16,18	4,8,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	3,5,7,12,17	4,8,9,11,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	3,5,7,12,16,18	4,8,9,11,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	3,5,7,12,17,18	4,8,9,11,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	3,5,7,12,16	4,8,9,11,15	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	3,5,7,12,14,18	4,8,9,11,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,7,12,14,16,17	4,8,9,11,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	3,5,7,12,14	4,8,9,11,15	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	3,5,7,12,14,16,17,18	4,8,9,11,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	3,5,7,12,17,18	4,8,9,11,13,17,18	2^{-34}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	3,5,7,12,16	4,8,9,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	3,5,7,12,17	4,8,9,11,13,15,17	2^{-34}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	3,5,7,12,16,18	4,8,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	3,5,7,12,14	4,8,9,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	3,5,7,12,14,16,17,18	4,8,9,11,13,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	3,5,7,12,14,18	4,8,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	3,5,7,12,14,16,17	4,8,9,11,13,15,17	2^{-23}

Table 0.479 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	3,5,7,10,17,18	4,8,9,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	3,5,7,10,16	4,8,9	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	3,5,7,10,17	4,8,9,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	3,5,7,10,16,18	4,8,9,15,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	3,5,7,10,14	4,8,9	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	3,5,7,10,14,16,17,18	4,8,9,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	3,5,7,10,14,18	4,8,9,15,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	3,5,7,10,14,16,17	4,8,9,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	3,5,7,10,17	4,8,9,13,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,7,10,16,18	4,8,9,13,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	3,5,7,10,17,18	4,8,9,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	3,5,7,10,16	4,8,9,13,15	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	3,5,7,10,14,18	4,8,9,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	3,5,7,10,14,16,17	4,8,9,13,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	3,5,7,10,14	4,8,9,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	3,5,7,10,14,16,17,18	4,8,9,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	3,5,7,10,12	4,8,9	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	3,5,7,10,12,16,17,18	4,8,9,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	3,5,7,10,12,18	4,8,9,15,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	3,5,7,10,12,16,17	4,8,9,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	3,5,7,10,12,14,17,18	4,8,9,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	3,5,7,10,12,14,16	4,8,9	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	3,5,7,10,12,14,17	4,8,9,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	3,5,7,10,12,14,16,18	4,8,9,15,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	3,5,7,10,12,18	4,8,9,13,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	3,5,7,10,12,16,17	4,8,9,13,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	3,5,7,10,12	4,8,9,13,15	$2^{-28.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	3,5,7,10,12,16,17,18	4,8,9,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	3,5,7,10,12,14,17	4,8,9,13,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	3,5,7,10,12,14,16,18	4,8,9,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	3,5,7,10,12,14,17,18	4,8,9,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	3,5,7,10,12,14,16	4,8,9,13,15	$2^{-17.5}$

Table 0.480 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	3,5,7,10,17	4,8,9,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	3,5,7,10,16,18	4,8,9,11,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	3,5,7,10,17,18	4,8,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	3,5,7,10,16	4,8,9,11,15	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	3,5,7,10,14,18	4,8,9,11,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	3,5,7,10,14,16,17	4,8,9,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	3,5,7,10,14	4,8,9,11,15	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	3,5,7,10,14,16,17,18	4,8,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	3,5,7,10,17,18	4,8,9,11,13,17,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	3,5,7,10,16	4,8,9,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	3,5,7,10,17	4,8,9,11,13,15,17	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	3,5,7,10,16,18	4,8,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,7,10,14	4,8,9,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	3,5,7,10,14,16,17,18	4,8,9,11,13,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,7,10,14,18	4,8,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	3,5,7,10,14,16,17	4,8,9,11,13,15,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	3,5,7,10,12,18	4,8,9,11,18	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	3,5,7,10,12,16,17	4,8,9,11,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	3,5,7,10,12	4,8,9,11,15	2^{-23}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	3,5,7,10,12,16,17,18	4,8,9,11,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	3,5,7,10,12,14,17	4,8,9,11,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	3,5,7,10,12,14,16,18	4,8,9,11,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	3,5,7,10,12,14,17,18	4,8,9,11,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	3,5,7,10,12,14,16	4,8,9,11,15	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	3,5,7,10,12	4,8,9,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	3,5,7,10,12,16,17,18	4,8,9,11,13,17,18	2^{-1}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	3,5,7,10,12,18	4,8,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	3,5,7,10,12,16,17	4,8,9,11,13,15,17	2^{-1}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	3,5,7,10,12,14,17,18	4,8,9,11,13,17,18	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	3,5,7,10,12,14,16	4,8,9,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	3,5,7,10,12,14,17	4,8,9,11,13,15,17	2^{-12}
$(0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	3,5,7,10,12,14,16,18	4,8,9,11,13,15,18	$2^{-17.5}$

Table 0.481 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	3,5	4,6	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	3,5,16,17,18	4,6,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	3,5,18	4,6,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	3,5,16,17	4,6,15,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	3,5,14,17,18	4,6,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	3,5,14,16	4,6	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	3,5,14,17	4,6,15,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	3,5,14,16,18	4,6,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	3,5,18	4,6,13,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	3,5,16,17	4,6,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	3,5	4,6,13,15	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	3,5,16,17,18	4,6,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,14,17	4,6,13,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	3,5,14,16,18	4,6,13,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,14,17,18	4,6,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	3,5,14,16	4,6,13,15	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	3,5,12,17,18	4,6,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	3,5,12,16	4,6	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	3,5,12,17	4,6,15,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	3,5,12,16,18	4,6,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	3,5,12,14	4,6	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	3,5,12,14,16,17,18	4,6,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	3,5,12,14,18	4,6,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	3,5,12,14,16,17	4,6,15,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	3,5,12,17	4,6,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	3,5,12,16,18	4,6,13,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	3,5,12,17,18	4,6,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	3,5,12,16	4,6,13,15	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	3,5,12,14,18	4,6,13,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	3,5,12,14,16,17	4,6,13,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	3,5,12,14	4,6,13,15	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	3,5,12,14,16,17,18	4,6,13,15,17,18	$2^{-28.5}$

Table 0.482 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	3,5,18	4,6,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	3,5,16,17	4,6,11,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	3,5	4,6,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	3,5,16,17,18	4,6,11,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	3,5,14,17	4,6,11,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	3,5,14,16,18	4,6,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	3,5,14,17,18	4,6,11,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	3,5,14,16	4,6,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	3,5	4,6,11,13	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	3,5,16,17,18	4,6,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	3,5,18	4,6,11,13,15,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	3,5,16,17	4,6,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	3,5,14,17,18	4,6,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	3,5,14,16	4,6,11,13	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	3,5,14,17	4,6,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	3,5,14,16,18	4,6,11,13,15,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,12,17	4,6,11,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	3,5,12,16,18	4,6,11,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,12,17,18	4,6,11,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	3,5,12,16	4,6,11,15	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	3,5,12,14,18	4,6,11,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5,12,14,16,17	4,6,11,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	3,5,12,14	4,6,11,15	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5,12,14,16,17,18	4,6,11,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,5,12,17,18	4,6,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,5,12,16	4,6,11,13	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	3,5,12,17	4,6,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	3,5,12,16,18	4,6,11,13,15,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	3,5,12,14	4,6,11,13	2^{-1}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	3,5,12,14,16,17,18	4,6,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	3,5,12,14,18	4,6,11,13,15,18	2^{-1}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	3,5,12,14,16,17	4,6,11,13,15,17	$2^{-17.5}$

Table 0.483 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	3,5,10,17,18	4,6,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	3,5,10,16	4,6	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	3,5,10,17	4,6,15,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	3,5,10,16,18	4,6,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	3,5,10,14	4,6	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	3,5,10,14,16,17,18	4,6,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	3,5,10,14,18	4,6,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	3,5,10,14,16,17	4,6,15,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	3,5,10,17	4,6,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	3,5,10,16,18	4,6,13,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	3,5,10,17,18	4,6,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	3,5,10,16	4,6,13,15	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	3,5,10,14,18	4,6,13,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	3,5,10,14,16,17	4,6,13,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	3,5,10,14	4,6,13,15	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	3,5,10,14,16,17,18	4,6,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	3,5,10,12	4,6	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	3,5,10,12,16,17,18	4,6,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	3,5,10,12,18	4,6,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	3,5,10,12,16,17	4,6,15,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	3,5,10,12,14,17,18	4,6,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	3,5,10,12,14,16	4,6	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	3,5,10,12,14,17	4,6,15,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	3,5,10,12,14,16,18	4,6,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	3,5,10,12,18	4,6,13,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	3,5,10,12,16,17	4,6,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	3,5,10,12	4,6,13,15	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	3,5,10,12,16,17,18	4,6,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	3,5,10,12,14,17	4,6,13,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	3,5,10,12,14,16,18	4,6,13,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	3,5,10,12,14,17,18	4,6,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	3,5,10,12,14,16	4,6,13,15	2^{-23}

Table 0.484 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	3,5,10,17	4,6,11,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,10,16,18	4,6,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	3,5,10,17,18	4,6,11,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,10,16	4,6,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	3,5,10,14,18	4,6,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	3,5,10,14,16,17	4,6,11,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	3,5,10,14	4,6,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	3,5,10,14,16,17,18	4,6,11,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	3,5,10,17,18	4,6,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	3,5,10,16	4,6,11,13	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	3,5,10,17	4,6,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	3,5,10,16,18	4,6,11,13,15,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	3,5,10,14	4,6,11,13	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	3,5,10,14,16,17,18	4,6,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	3,5,10,14,18	4,6,11,13,15,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	3,5,10,14,16,17	4,6,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	3,5,10,12,18	4,6,11,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	3,5,10,12,16,17	4,6,11,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	3,5,10,12	4,6,11,15	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	3,5,10,12,16,17,18	4,6,11,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,10,12,14,17	4,6,11,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	3,5,10,12,14,16,18	4,6,11,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	3,5,10,12,14,17,18	4,6,11,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	3,5,10,12,14,16	4,6,11,15	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	3,5,10,12	4,6,11,13	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	3,5,10,12,16,17,18	4,6,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	3,5,10,12,18	4,6,11,13,15,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	3,5,10,12,16,17	4,6,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	3,5,10,12,14,17,18	4,6,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	3,5,10,12,14,16	4,6,11,13	2^{-34}
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	3,5,10,12,14,17	4,6,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	3,5,10,12,14,16,18	4,6,11,13,15,18	2^{-34}

Table 0.485 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	3,5,18	4,6,9,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	3,5,16,17	4,6,9,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	3,5	4,6,9,15	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,5,16,17,18	4,6,9,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	3,5,14,17	4,6,9,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	3,5,14,16,18	4,6,9,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	3,5,14,17,18	4,6,9,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	3,5,14,16	4,6,9,15	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	3,5	4,6,9,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	3,5,16,17,18	4,6,9,13,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	3,5,18	4,6,9,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	3,5,16,17	4,6,9,13,15,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	3,5,14,17,18	4,6,9,13,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	3,5,14,16	4,6,9,13	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	3,5,14,17	4,6,9,13,15,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	3,5,14,16,18	4,6,9,13,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	3,5,12,17	4,6,9,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	3,5,12,16,18	4,6,9,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	3,5,12,17,18	4,6,9,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	3,5,12,16	4,6,9,15	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	3,5,12,14,18	4,6,9,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	3,5,12,14,16,17	4,6,9,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	3,5,12,14	4,6,9,15	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	3,5,12,14,16,17,18	4,6,9,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,12,17,18	4,6,9,13,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	3,5,12,16	4,6,9,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,12,17	4,6,9,13,15,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	3,5,12,16,18	4,6,9,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	3,5,12,14	4,6,9,13	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	3,5,12,14,16,17,18	4,6,9,13,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	3,5,12,14,18	4,6,9,13,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	3,5,12,14,16,17	4,6,9,13,15,17	2^{-23}

Table 0.486 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	3,5	4,6,9,11	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	3,5,16,17,18	4,6,9,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	3,5,18	4,6,9,11,15,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	3,5,16,17	4,6,9,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	3,5,14,17,18	4,6,9,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	3,5,14,16	4,6,9,11	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	3,5,14,17	4,6,9,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	3,5,14,16,18	4,6,9,11,15,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	3,5,18	4,6,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	3,5,16,17	4,6,9,11,13,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	3,5	4,6,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	3,5,16,17,18	4,6,9,11,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	3,5,14,17	4,6,9,11,13,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	3,5,14,16,18	4,6,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	3,5,14,17,18	4,6,9,11,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	3,5,14,16	4,6,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	3,5,12,17,18	4,6,9,11,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,12,16	4,6,9,11	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	3,5,12,17	4,6,9,11,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,12,16,18	4,6,9,11,15,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	3,5,12,14	4,6,9,11	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	3,5,12,14,16,17,18	4,6,9,11,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	3,5,12,14,18	4,6,9,11,15,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	3,5,12,14,16,17	4,6,9,11,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	3,5,12,17	4,6,9,11,13,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	3,5,12,16,18	4,6,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	3,5,12,17,18	4,6,9,11,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	3,5,12,16	4,6,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	3,5,12,14,18	4,6,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	3,5,12,14,16,17	4,6,9,11,13,17	2^{-34}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	3,5,12,14	4,6,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	3,5,12,14,16,17,18	4,6,9,11,13,15,17,18	2^{-34}

Table 0.487 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	3,5,10,17	4,6,9,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	3,5,10,16,18	4,6,9,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	3,5,10,17,18	4,6,9,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	3,5,10,16	4,6,9,15	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	3,5,10,14,18	4,6,9,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	3,5,10,14,16,17	4,6,9,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	3,5,10,14	4,6,9,15	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	3,5,10,14,16,17,18	4,6,9,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	3,5,10,17,18	4,6,9,13,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,5,10,16	4,6,9,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	3,5,10,17	4,6,9,13,15,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	3,5,10,16,18	4,6,9,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	3,5,10,14	4,6,9,13	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	3,5,10,14,16,17,18	4,6,9,13,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	3,5,10,14,18	4,6,9,13,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	3,5,10,14,16,17	4,6,9,13,15,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	3,5,10,12,18	4,6,9,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	3,5,10,12,16,17	4,6,9,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	3,5,10,12	4,6,9,15	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	3,5,10,12,16,17,18	4,6,9,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	3,5,10,12,14,17	4,6,9,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	3,5,10,12,14,16,18	4,6,9,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	3,5,10,12,14,17,18	4,6,9,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	3,5,10,12,14,16	4,6,9,15	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	3,5,10,12	4,6,9,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,10,12,16,17,18	4,6,9,13,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	3,5,10,12,18	4,6,9,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,10,12,16,17	4,6,9,13,15,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	3,5,10,12,14,17,18	4,6,9,13,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	3,5,10,12,14,16	4,6,9,13	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	3,5,10,12,14,17	4,6,9,13,15,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	3,5,10,12,14,16,18	4,6,9,13,15,18	$2^{-28.5}$

Table 0.488 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	3,5,10,17,18	4,6,9,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	3,5,10,16	4,6,9,11	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	3,5,10,17	4,6,9,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	3,5,10,16,18	4,6,9,11,15,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	3,5,10,14	4,6,9,11	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	3,5,10,14,16,17,18	4,6,9,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	3,5,10,14,18	4,6,9,11,15,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	3,5,10,14,16,17	4,6,9,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	3,5,10,17	4,6,9,11,13,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	3,5,10,16,18	4,6,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	3,5,10,17,18	4,6,9,11,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	3,5,10,16	4,6,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	3,5,10,14,18	4,6,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	3,5,10,14,16,17	4,6,9,11,13,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	3,5,10,14	4,6,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	3,5,10,14,16,17,18	4,6,9,11,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	3,5,10,12	4,6,9,11	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	3,5,10,12,16,17,18	4,6,9,11,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	3,5,10,12,18	4,6,9,11,15,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	3,5,10,12,16,17	4,6,9,11,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	3,5,10,12,14,17,18	4,6,9,11,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	3,5,10,12,14,16	4,6,9,11	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	3,5,10,12,14,17	4,6,9,11,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	3,5,10,12,14,16,18	4,6,9,11,15,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	3,5,10,12,18	4,6,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	3,5,10,12,16,17	4,6,9,11,13,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	3,5,10,12	4,6,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	3,5,10,12,16,17,18	4,6,9,11,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	3,5,10,12,14,17	4,6,9,11,13,17	2^{-1}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	3,5,10,12,14,16,18	4,6,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	3,5,10,12,14,17,18	4,6,9,11,13,15,17,18	2^{-1}
$(0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	3,5,10,12,14,16	4,6,9,11,13,15	$2^{-17.5}$

Table 0.489 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	3,5,17,18	4,6,8,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	3,5,16	4,6,8	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	3,5,17	4,6,8,15,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	3,5,16,18	4,6,8,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	3,5,14	4,6,8	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	3,5,14,16,17,18	4,6,8,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	3,5,14,18	4,6,8,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	3,5,14,16,17	4,6,8,15,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,5,17	4,6,8,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	3,5,16,18	4,6,8,13,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	3,5,17,18	4,6,8,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	3,5,16	4,6,8,13,15	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	3,5,14,18	4,6,8,13,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	3,5,14,16,17	4,6,8,13,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	3,5,14	4,6,8,13,15	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	3,5,14,16,17,18	4,6,8,13,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	3,5,12	4,6,8	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	3,5,12,16,17,18	4,6,8,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	3,5,12,18	4,6,8,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	3,5,12,16,17	4,6,8,15,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	3,5,12,14,17,18	4,6,8,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	3,5,12,14,16	4,6,8	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	3,5,12,14,17	4,6,8,15,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	3,5,12,14,16,18	4,6,8,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,12,18	4,6,8,13,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	3,5,12,16,17	4,6,8,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,12	4,6,8,13,15	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	3,5,12,16,17,18	4,6,8,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	3,5,12,14,17	4,6,8,13,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	3,5,12,14,16,18	4,6,8,13,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	3,5,12,14,17,18	4,6,8,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	3,5,12,14,16	4,6,8,13,15	2^{-12}

Table 0.490 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	3,5,17	4,6,8,11,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	3,5,16,18	4,6,8,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	3,5,17,18	4,6,8,11,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	3,5,16	4,6,8,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	3,5,14,18	4,6,8,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	3,5,14,16,17	4,6,8,11,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	3,5,14	4,6,8,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	3,5,14,16,17,18	4,6,8,11,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	3,5,17,18	4,6,8,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	3,5,16	4,6,8,11,13	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	3,5,17	4,6,8,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	3,5,16,18	4,6,8,11,13,15,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	3,5,14	4,6,8,11,13	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	3,5,14,16,17,18	4,6,8,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	3,5,14,18	4,6,8,11,13,15,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	3,5,14,16,17	4,6,8,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	3,5,12,18	4,6,8,11,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	3,5,12,16,17	4,6,8,11,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	3,5,12	4,6,8,11,15	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	3,5,12,16,17,18	4,6,8,11,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	3,5,12,14,17	4,6,8,11,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	3,5,12,14,16,18	4,6,8,11,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	3,5,12,14,17,18	4,6,8,11,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	3,5,12,14,16	4,6,8,11,15	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	3,5,12	4,6,8,11,13	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	3,5,12,16,17,18	4,6,8,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	3,5,12,18	4,6,8,11,13,15,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	3,5,12,16,17	4,6,8,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	3,5,12,14,17,18	4,6,8,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	3,5,12,14,16	4,6,8,11,13	2^{-1}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	3,5,12,14,17	4,6,8,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	3,5,12,14,16,18	4,6,8,11,13,15,18	2^{-1}

Table 0.491 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	3,5,10	4,6,8	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	3,5,10,16,17,18	4,6,8,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	3,5,10,18	4,6,8,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	3,5,10,16,17	4,6,8,15,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	3,5,10,14,17,18	4,6,8,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	3,5,10,14,16	4,6,8	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	3,5,10,14,17	4,6,8,15,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	3,5,10,14,16,18	4,6,8,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	3,5,10,18	4,6,8,13,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	3,5,10,16,17	4,6,8,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	3,5,10	4,6,8,13,15	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	3,5,10,16,17,18	4,6,8,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	3,5,10,14,17	4,6,8,13,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	3,5,10,14,16,18	4,6,8,13,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	3,5,10,14,17,18	4,6,8,13,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	3,5,10,14,16	4,6,8,13,15	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	3,5,10,12,17,18	4,6,8,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	3,5,10,12,16	4,6,8	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	3,5,10,12,17	4,6,8,15,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	3,5,10,12,16,18	4,6,8,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	3,5,10,12,14	4,6,8	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	3,5,10,12,14,16,17,18	4,6,8,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	3,5,10,12,14,18	4,6,8,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	3,5,10,12,14,16,17	4,6,8,15,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	3,5,10,12,17	4,6,8,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,10,12,16,18	4,6,8,13,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	3,5,10,12,17,18	4,6,8,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,10,12,16	4,6,8,13,15	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	3,5,10,12,14,18	4,6,8,13,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	3,5,10,12,14,16,17	4,6,8,13,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	3,5,10,12,14	4,6,8,13,15	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	3,5,10,12,14,16,17,18	4,6,8,13,15,17,18	$2^{-6.5}$

Table 0.492 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	3,5,10,18	4,6,8,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	3,5,10,16,17	4,6,8,11,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	3,5,10	4,6,8,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	3,5,10,16,17,18	4,6,8,11,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	3,5,10,14,17	4,6,8,11,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	3,5,10,14,16,18	4,6,8,11,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	3,5,10,14,17,18	4,6,8,11,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	3,5,10,14,16	4,6,8,11,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	3,5,10	4,6,8,11,13	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	3,5,10,16,17,18	4,6,8,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	3,5,10,18	4,6,8,11,13,15,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	3,5,10,16,17	4,6,8,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	3,5,10,14,17,18	4,6,8,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	3,5,10,14,16	4,6,8,11,13	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	3,5,10,14,17	4,6,8,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	3,5,10,14,16,18	4,6,8,11,13,15,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	3,5,10,12,17	4,6,8,11,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	3,5,10,12,16,18	4,6,8,11,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	3,5,10,12,17,18	4,6,8,11,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	3,5,10,12,16	4,6,8,11,15	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	3,5,10,12,14,18	4,6,8,11,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	3,5,10,12,14,16,17	4,6,8,11,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	3,5,10,12,14	4,6,8,11,15	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	3,5,10,12,14,16,17,18	4,6,8,11,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	3,5,10,12,17,18	4,6,8,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	3,5,10,12,16	4,6,8,11,13	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	3,5,10,12,17	4,6,8,11,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	3,5,10,12,16,18	4,6,8,11,13,15,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	3,5,10,12,14	4,6,8,11,13	2^{-34}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	3,5,10,12,14,16,17,18	4,6,8,11,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	3,5,10,12,14,18	4,6,8,11,13,15,18	2^{-34}
$(0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	3,5,10,12,14,16,17	4,6,8,11,13,15,17	$2^{-17.5}$

Table 0.493 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	3,5,17	4,6,8,9,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	3,5,16,18	4,6,8,9,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	3,5,17,18	4,6,8,9,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	3,5,16	4,6,8,9,15	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	3,5,14,18	4,6,8,9,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	3,5,14,16,17	4,6,8,9,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	3,5,14	4,6,8,9,15	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	3,5,14,16,17,18	4,6,8,9,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	3,5,17,18	4,6,8,9,13,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	3,5,16	4,6,8,9,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	3,5,17	4,6,8,9,13,15,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	3,5,16,18	4,6,8,9,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	3,5,14	4,6,8,9,13	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	3,5,14,16,17,18	4,6,8,9,13,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	3,5,14,18	4,6,8,9,13,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	3,5,14,16,17	4,6,8,9,13,15,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	3,5,12,18	4,6,8,9,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	3,5,12,16,17	4,6,8,9,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	3,5,12	4,6,8,9,15	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	3,5,12,16,17,18	4,6,8,9,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	3,5,12,14,17	4,6,8,9,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	3,5,12,14,16,18	4,6,8,9,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	3,5,12,14,17,18	4,6,8,9,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	3,5,12,14,16	4,6,8,9,15	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	3,5,12	4,6,8,9,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	3,5,12,16,17,18	4,6,8,9,13,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	3,5,12,18	4,6,8,9,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	3,5,12,16,17	4,6,8,9,13,15,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	3,5,12,14,17,18	4,6,8,9,13,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	3,5,12,14,16	4,6,8,9,13	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	3,5,12,14,17	4,6,8,9,13,15,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	3,5,12,14,16,18	4,6,8,9,13,15,18	$2^{-6.5}$

Table 0.494 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,17,18	4,6,8,9,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	3,5,16	4,6,8,9,11	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,17	4,6,8,9,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	3,5,16,18	4,6,8,9,11,15,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	3,5,14	4,6,8,9,11	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	3,5,14,16,17,18	4,6,8,9,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	3,5,14,18	4,6,8,9,11,15,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	3,5,14,16,17	4,6,8,9,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	3,5,17	4,6,8,9,11,13,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	3,5,16,18	4,6,8,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	3,5,17,18	4,6,8,9,11,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	3,5,16	4,6,8,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	3,5,14,18	4,6,8,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	3,5,14,16,17	4,6,8,9,11,13,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	3,5,14	4,6,8,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	3,5,14,16,17,18	4,6,8,9,11,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	3,5,12	4,6,8,9,11	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	3,5,12,16,17,18	4,6,8,9,11,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	3,5,12,18	4,6,8,9,11,15,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	3,5,12,16,17	4,6,8,9,11,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	3,5,12,14,17,18	4,6,8,9,11,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	3,5,12,14,16	4,6,8,9,11	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	3,5,12,14,17	4,6,8,9,11,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	3,5,12,14,16,18	4,6,8,9,11,15,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	3,5,12,18	4,6,8,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	3,5,12,16,17	4,6,8,9,11,13,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	3,5,12	4,6,8,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	3,5,12,16,17,18	4,6,8,9,11,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	3,5,12,14,17	4,6,8,9,11,13,17	2^{-34}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	3,5,12,14,16,18	4,6,8,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	3,5,12,14,17,18	4,6,8,9,11,13,15,17,18	2^{-34}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	3,5,12,14,16	4,6,8,9,11,13,15	$2^{-17.5}$

Table 0.495 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	3,5,10,18	4,6,8,9,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	3,5,10,16,17	4,6,8,9,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	3,5,10	4,6,8,9,15	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	3,5,10,16,17,18	4,6,8,9,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	3,5,10,14,17	4,6,8,9,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	3,5,10,14,16,18	4,6,8,9,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	3,5,10,14,17,18	4,6,8,9,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	3,5,10,14,16	4,6,8,9,15	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	3,5,10	4,6,8,9,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	3,5,10,16,17,18	4,6,8,9,13,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	3,5,10,18	4,6,8,9,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	3,5,10,16,17	4,6,8,9,13,15,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	3,5,10,14,17,18	4,6,8,9,13,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,10,14,16	4,6,8,9,13	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	3,5,10,14,17	4,6,8,9,13,15,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,10,14,16,18	4,6,8,9,13,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	3,5,10,12,17	4,6,8,9,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	3,5,10,12,16,18	4,6,8,9,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	3,5,10,12,17,18	4,6,8,9,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	3,5,10,12,16	4,6,8,9,15	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	3,5,10,12,14,18	4,6,8,9,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	3,5,10,12,14,16,17	4,6,8,9,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	3,5,10,12,14	4,6,8,9,15	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	3,5,10,12,14,16,17,18	4,6,8,9,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	3,5,10,12,17,18	4,6,8,9,13,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	3,5,10,12,16	4,6,8,9,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	3,5,10,12,17	4,6,8,9,13,15,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	3,5,10,12,16,18	4,6,8,9,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	3,5,10,12,14	4,6,8,9,13	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	3,5,10,12,14,16,17,18	4,6,8,9,13,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	3,5,10,12,14,18	4,6,8,9,13,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	3,5,10,12,14,16,17	4,6,8,9,13,15,17	2^{-12}

Table 0.496 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	3,5,10	4,6,8,9,11	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	3,5,10,16,17,18	4,6,8,9,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	3,5,10,18	4,6,8,9,11,15,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	3,5,10,16,17	4,6,8,9,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	3,5,10,14,17,18	4,6,8,9,11,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	3,5,10,14,16	4,6,8,9,11	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	3,5,10,14,17	4,6,8,9,11,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	3,5,10,14,16,18	4,6,8,9,11,15,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	3,5,10,18	4,6,8,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	3,5,10,16,17	4,6,8,9,11,13,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	3,5,10	4,6,8,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	3,5,10,16,17,18	4,6,8,9,11,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	3,5,10,14,17	4,6,8,9,11,13,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	3,5,10,14,16,18	4,6,8,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	3,5,10,14,17,18	4,6,8,9,11,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	3,5,10,14,16	4,6,8,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	3,5,10,12,17,18	4,6,8,9,11,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,10,12,16	4,6,8,9,11	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	3,5,10,12,17	4,6,8,9,11,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,10,12,16,18	4,6,8,9,11,15,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5,10,12,14	4,6,8,9,11	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	3,5,10,12,14,16,17,18	4,6,8,9,11,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5,10,12,14,18	4,6,8,9,11,15,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	3,5,10,12,14,16,17	4,6,8,9,11,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,5,10,12,17	4,6,8,9,11,13,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,5,10,12,16,18	4,6,8,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	3,5,10,12,17,18	4,6,8,9,11,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	3,5,10,12,16	4,6,8,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	3,5,10,12,14,18	4,6,8,9,11,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	3,5,10,12,14,16,17	4,6,8,9,11,13,17	2^{-1}
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	3,5,10,12,14	4,6,8,9,11,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	3,5,10,12,14,16,17,18	4,6,8,9,11,13,15,17,18	2^{-1}

Table 0.497 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	3,5,7,18	4,6,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	3,5,7,16,17	4,6,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	3,5,7	4,6,15	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	3,5,7,16,17,18	4,6,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	3,5,7,14,17	4,6,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	3,5,7,14,16,18	4,6,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	3,5,7,14,17,18	4,6,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	3,5,7,14,16	4,6,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	3,5,7	4,6,13	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	3,5,7,16,17,18	4,6,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	3,5,7,18	4,6,13,15,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	3,5,7,16,17	4,6,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	3,5,7,14,17,18	4,6,13,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	3,5,7,14,16	4,6,13	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	3,5,7,14,17	4,6,13,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	3,5,7,14,16,18	4,6,13,15,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	3,5,7,12,17	4,6,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	3,5,7,12,16,18	4,6,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	3,5,7,12,17,18	4,6,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	3,5,7,12,16	4,6,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	3,5,7,12,14,18	4,6,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	3,5,7,12,14,16,17	4,6,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	3,5,7,12,14	4,6,15	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	3,5,7,12,14,16,17,18	4,6,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	3,5,7,12,17,18	4,6,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	3,5,7,12,16	4,6,13	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	3,5,7,12,17	4,6,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	3,5,7,12,16,18	4,6,13,15,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	3,5,7,12,14	4,6,13	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	3,5,7,12,14,16,17,18	4,6,13,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	3,5,7,12,14,18	4,6,13,15,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	3,5,7,12,14,16,17	4,6,13,15,17	$2^{-28.5}$

Table 0.498 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	3,5,7	4,6,11	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	3,5,7,16,17,18	4,6,11,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	3,5,7,18	4,6,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	3,5,7,16,17	4,6,11,15,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	3,5,7,14,17,18	4,6,11,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	3,5,7,14,16	4,6,11	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	3,5,7,14,17	4,6,11,15,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	3,5,7,14,16,18	4,6,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	3,5,7,18	4,6,11,13,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	3,5,7,16,17	4,6,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	3,5,7	4,6,11,13,15	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	3,5,7,16,17,18	4,6,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	3,5,7,14,17	4,6,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	3,5,7,14,16,18	4,6,11,13,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	3,5,7,14,17,18	4,6,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	3,5,7,14,16	4,6,11,13,15	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	3,5,7,12,17,18	4,6,11,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	3,5,7,12,16	4,6,11	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	3,5,7,12,17	4,6,11,15,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	3,5,7,12,16,18	4,6,11,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	3,5,7,12,14	4,6,11	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	3,5,7,12,14,16,17,18	4,6,11,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	3,5,7,12,14,18	4,6,11,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	3,5,7,12,14,16,17	4,6,11,15,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,7,12,17	4,6,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	3,5,7,12,16,18	4,6,11,13,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,7,12,17,18	4,6,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	3,5,7,12,16	4,6,11,13,15	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	3,5,7,12,14,18	4,6,11,13,18	2^{-1}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	3,5,7,12,14,16,17	4,6,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	3,5,7,12,14	4,6,11,13,15	2^{-1}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	3,5,7,12,14,16,17,18	4,6,11,13,15,17,18	$2^{-17.5}$

Table 0.499 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	3,5,7,10,17	4,6,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	3,5,7,10,16,18	4,6,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	3,5,7,10,17,18	4,6,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	3,5,7,10,16	4,6,15	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	3,5,7,10,14,18	4,6,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	3,5,7,10,14,16,17	4,6,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	3,5,7,10,14	4,6,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	3,5,7,10,14,16,17,18	4,6,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	3,5,7,10,17,18	4,6,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	3,5,7,10,16	4,6,13	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	3,5,7,10,17	4,6,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	3,5,7,10,16,18	4,6,13,15,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	3,5,7,10,14	4,6,13	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	3,5,7,10,14,16,17,18	4,6,13,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	3,5,7,10,14,18	4,6,13,15,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	3,5,7,10,14,16,17	4,6,13,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	3,5,7,10,12,18	4,6,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	3,5,7,10,12,16,17	4,6,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	3,5,7,10,12	4,6,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	3,5,7,10,12,16,17,18	4,6,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	3,5,7,10,12,14,17	4,6,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	3,5,7,10,12,14,16,18	4,6,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	3,5,7,10,12,14,17,18	4,6,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	3,5,7,10,12,14,16	4,6,15	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	3,5,7,10,12	4,6,13	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	3,5,7,10,12,16,17,18	4,6,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	3,5,7,10,12,18	4,6,13,15,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	3,5,7,10,12,16,17	4,6,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	3,5,7,10,12,14,17,18	4,6,13,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	3,5,7,10,12,14,16	4,6,13	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	3,5,7,10,12,14,17	4,6,13,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	3,5,7,10,12,14,16,18	4,6,13,15,18	2^{-23}

Table 0.500 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	3,5,7,10,17,18	4,6,11,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	3,5,7,10,16	4,6,11	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	3,5,7,10,17	4,6,11,15,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	3,5,7,10,16,18	4,6,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	3,5,7,10,14	4,6,11	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	3,5,7,10,14,16,17,18	4,6,11,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	3,5,7,10,14,18	4,6,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	3,5,7,10,14,16,17	4,6,11,15,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	3,5,7,10,17	4,6,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	3,5,7,10,16,18	4,6,11,13,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	3,5,7,10,17,18	4,6,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	3,5,7,10,16	4,6,11,13,15	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	3,5,7,10,14,18	4,6,11,13,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	3,5,7,10,14,16,17	4,6,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	3,5,7,10,14	4,6,11,13,15	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	3,5,7,10,14,16,17,18	4,6,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	3,5,7,10,12	4,6,11	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	3,5,7,10,12,16,17,18	4,6,11,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	3,5,7,10,12,18	4,6,11,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	3,5,7,10,12,16,17	4,6,11,15,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	3,5,7,10,12,14,17,18	4,6,11,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	3,5,7,10,12,14,16	4,6,11	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	3,5,7,10,12,14,17	4,6,11,15,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	3,5,7,10,12,14,16,18	4,6,11,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	3,5,7,10,12,18	4,6,11,13,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,7,10,12,16,17	4,6,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	3,5,7,10,12	4,6,11,13,15	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,7,10,12,16,17,18	4,6,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	3,5,7,10,12,14,17	4,6,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	3,5,7,10,12,14,16,18	4,6,11,13,18	2^{-34}
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	3,5,7,10,12,14,17,18	4,6,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	3,5,7,10,12,14,16	4,6,11,13,15	2^{-34}

Table 0.501 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	3,5,7	4,6,9	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	3,5,7,16,17,18	4,6,9,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	3,5,7,18	4,6,9,15,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	3,5,7,16,17	4,6,9,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	3,5,7,14,17,18	4,6,9,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	3,5,7,14,16	4,6,9	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	3,5,7,14,17	4,6,9,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	3,5,7,14,16,18	4,6,9,15,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	3,5,7,18	4,6,9,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	3,5,7,16,17	4,6,9,13,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	3,5,7	4,6,9,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	3,5,7,16,17,18	4,6,9,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	3,5,7,14,17	4,6,9,13,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	3,5,7,14,16,18	4,6,9,13,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	3,5,7,14,17,18	4,6,9,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	3,5,7,14,16	4,6,9,13,15	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,12,17,18	4,6,9,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	3,5,7,12,16	4,6,9	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,12,17	4,6,9,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	3,5,7,12,16,18	4,6,9,15,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	3,5,7,12,14	4,6,9	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5,7,12,14,16,17,18	4,6,9,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	3,5,7,12,14,18	4,6,9,15,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5,7,12,14,16,17	4,6,9,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	3,5,7,12,17	4,6,9,13,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	3,5,7,12,16,18	4,6,9,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,5,7,12,17,18	4,6,9,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,5,7,12,16	4,6,9,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	3,5,7,12,14,18	4,6,9,13,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	3,5,7,12,14,16,17	4,6,9,13,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	3,5,7,12,14	4,6,9,13,15	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	3,5,7,12,14,16,17,18	4,6,9,13,15,17,18	2^{-23}

Table 0.502 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	3,5,7,18	4,6,9,11,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,7,16,17	4,6,9,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	3,5,7	4,6,9,11,15	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	3,5,7,16,17,18	4,6,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	3,5,7,14,17	4,6,9,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	3,5,7,14,16,18	4,6,9,11,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	3,5,7,14,17,18	4,6,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	3,5,7,14,16	4,6,9,11,15	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	3,5,7	4,6,9,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	3,5,7,16,17,18	4,6,9,11,13,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	3,5,7,18	4,6,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	3,5,7,16,17	4,6,9,11,13,15,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,7,14,17,18	4,6,9,11,13,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	3,5,7,14,16	4,6,9,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,7,14,17	4,6,9,11,13,15,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	3,5,7,14,16,18	4,6,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	3,5,7,12,17	4,6,9,11,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	3,5,7,12,16,18	4,6,9,11,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	3,5,7,12,17,18	4,6,9,11,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	3,5,7,12,16	4,6,9,11,15	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	3,5,7,12,14,18	4,6,9,11,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	3,5,7,12,14,16,17	4,6,9,11,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	3,5,7,12,14	4,6,9,11,15	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	3,5,7,12,14,16,17,18	4,6,9,11,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	3,5,7,12,17,18	4,6,9,11,13,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	3,5,7,12,16	4,6,9,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	3,5,7,12,17	4,6,9,11,13,15,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	3,5,7,12,16,18	4,6,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	3,5,7,12,14	4,6,9,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	3,5,7,12,14,16,17,18	4,6,9,11,13,17,18	2^{-34}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	3,5,7,12,14,18	4,6,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	3,5,7,12,14,16,17	4,6,9,11,13,15,17	2^{-34}

Table 0.503 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	3,5,7,10,17,18	4,6,9,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,10,16	4,6,9	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	3,5,7,10,17	4,6,9,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,10,16,18	4,6,9,15,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,10,14	4,6,9	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	3,5,7,10,14,16,17,18	4,6,9,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,10,14,18	4,6,9,15,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	3,5,7,10,14,16,17	4,6,9,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	3,5,7,10,17	4,6,9,13,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	3,5,7,10,16,18	4,6,9,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	3,5,7,10,17,18	4,6,9,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	3,5,7,10,16	4,6,9,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	3,5,7,10,14,18	4,6,9,13,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	3,5,7,10,14,16,17	4,6,9,13,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	3,5,7,10,14	4,6,9,13,15	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	3,5,7,10,14,16,17,18	4,6,9,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	3,5,7,10,12	4,6,9	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	3,5,7,10,12,16,17,18	4,6,9,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	3,5,7,10,12,18	4,6,9,15,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	3,5,7,10,12,16,17	4,6,9,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	3,5,7,10,12,14,17,18	4,6,9,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	3,5,7,10,12,14,16	4,6,9	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	3,5,7,10,12,14,17	4,6,9,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	3,5,7,10,12,14,16,18	4,6,9,15,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	3,5,7,10,12,18	4,6,9,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	3,5,7,10,12,16,17	4,6,9,13,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	3,5,7,10,12	4,6,9,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	3,5,7,10,12,16,17,18	4,6,9,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	3,5,7,10,12,14,17	4,6,9,13,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	3,5,7,10,12,14,16,18	4,6,9,13,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	3,5,7,10,12,14,17,18	4,6,9,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	3,5,7,10,12,14,16	4,6,9,13,15	$2^{-28.5}$

Table 0.504 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	3,5,7,10,17	4,6,9,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	3,5,7,10,16,18	4,6,9,11,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	3,5,7,10,17,18	4,6,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	3,5,7,10,16	4,6,9,11,15	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	3,5,7,10,14,18	4,6,9,11,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	3,5,7,10,14,16,17	4,6,9,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	3,5,7,10,14	4,6,9,11,15	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	3,5,7,10,14,16,17,18	4,6,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	3,5,7,10,17,18	4,6,9,11,13,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	3,5,7,10,16	4,6,9,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	3,5,7,10,17	4,6,9,11,13,15,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	3,5,7,10,16,18	4,6,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	3,5,7,10,14	4,6,9,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	3,5,7,10,14,16,17,18	4,6,9,11,13,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	3,5,7,10,14,18	4,6,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	3,5,7,10,14,16,17	4,6,9,11,13,15,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	3,5,7,10,12,18	4,6,9,11,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	3,5,7,10,12,16,17	4,6,9,11,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	3,5,7,10,12	4,6,9,11,15	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	3,5,7,10,12,16,17,18	4,6,9,11,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	3,5,7,10,12,14,17	4,6,9,11,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	3,5,7,10,12,14,16,18	4,6,9,11,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	3,5,7,10,12,14,17,18	4,6,9,11,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	3,5,7,10,12,14,16	4,6,9,11,15	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	3,5,7,10,12	4,6,9,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	3,5,7,10,12,16,17,18	4,6,9,11,13,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	3,5,7,10,12,18	4,6,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	3,5,7,10,12,16,17	4,6,9,11,13,15,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	3,5,7,10,12,14,17,18	4,6,9,11,13,17,18	2^{-1}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	3,5,7,10,12,14,16	4,6,9,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	3,5,7,10,12,14,17	4,6,9,11,13,15,17	2^{-1}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	3,5,7,10,12,14,16,18	4,6,9,11,13,15,18	$2^{-17.5}$

Table 0.505 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,17	4,6,8,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	3,5,7,16,18	4,6,8,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,17,18	4,6,8,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	3,5,7,16	4,6,8,15	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	3,5,7,14,18	4,6,8,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,14,16,17	4,6,8,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	3,5,7,14	4,6,8,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,14,16,17,18	4,6,8,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	3,5,7,17,18	4,6,8,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	3,5,7,16	4,6,8,13	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	3,5,7,17	4,6,8,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	3,5,7,16,18	4,6,8,13,15,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	3,5,7,14	4,6,8,13	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	3,5,7,14,16,17,18	4,6,8,13,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	3,5,7,14,18	4,6,8,13,15,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	3,5,7,14,16,17	4,6,8,13,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	3,5,7,12,18	4,6,8,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	3,5,7,12,16,17	4,6,8,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	3,5,7,12	4,6,8,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	3,5,7,12,16,17,18	4,6,8,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	3,5,7,12,14,17	4,6,8,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	3,5,7,12,14,16,18	4,6,8,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	3,5,7,12,14,17,18	4,6,8,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	3,5,7,12,14,16	4,6,8,15	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	3,5,7,12	4,6,8,13	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	3,5,7,12,16,17,18	4,6,8,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	3,5,7,12,18	4,6,8,13,15,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	3,5,7,12,16,17	4,6,8,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	3,5,7,12,14,17,18	4,6,8,13,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	3,5,7,12,14,16	4,6,8,13	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	3,5,7,12,14,17	4,6,8,13,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	3,5,7,12,14,16,18	4,6,8,13,15,18	2^{-12}

Table 0.506 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	3,5,7,17,18	4,6,8,11,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	3,5,7,16	4,6,8,11	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	3,5,7,17	4,6,8,11,15,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	3,5,7,16,18	4,6,8,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	3,5,7,14	4,6,8,11	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	3,5,7,14,16,17,18	4,6,8,11,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	3,5,7,14,18	4,6,8,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	3,5,7,14,16,17	4,6,8,11,15,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	3,5,7,17	4,6,8,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	3,5,7,16,18	4,6,8,11,13,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	3,5,7,17,18	4,6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	3,5,7,16	4,6,8,11,13,15	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	3,5,7,14,18	4,6,8,11,13,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	3,5,7,14,16,17	4,6,8,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	3,5,7,14	4,6,8,11,13,15	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	3,5,7,14,16,17,18	4,6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	3,5,7,12	4,6,8,11	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	3,5,7,12,16,17,18	4,6,8,11,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	3,5,7,12,18	4,6,8,11,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	3,5,7,12,16,17	4,6,8,11,15,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	3,5,7,12,14,17,18	4,6,8,11,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	3,5,7,12,14,16	4,6,8,11	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	3,5,7,12,14,17	4,6,8,11,15,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	3,5,7,12,14,16,18	4,6,8,11,15,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	3,5,7,12,18	4,6,8,11,13,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	3,5,7,12,16,17	4,6,8,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	3,5,7,12	4,6,8,11,13,15	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	3,5,7,12,16,17,18	4,6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	3,5,7,12,14,17	4,6,8,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	3,5,7,12,14,16,18	4,6,8,11,13,18	2^{-1}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	3,5,7,12,14,17,18	4,6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	3,5,7,12,14,16	4,6,8,11,13,15	2^{-1}

Table 0.507 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	3,5,7,10,18	4,6,8,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	3,5,7,10,16,17	4,6,8,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	3,5,7,10	4,6,8,15	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	3,5,7,10,16,17,18	4,6,8,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	3,5,7,10,14,17	4,6,8,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	3,5,7,10,14,16,18	4,6,8,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	3,5,7,10,14,17,18	4,6,8,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	3,5,7,10,14,16	4,6,8,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	3,5,7,10	4,6,8,13	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	3,5,7,10,16,17,18	4,6,8,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	3,5,7,10,18	4,6,8,13,15,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	3,5,7,10,16,17	4,6,8,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	3,5,7,10,14,17,18	4,6,8,13,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	3,5,7,10,14,16	4,6,8,13	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	3,5,7,10,14,17	4,6,8,13,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	3,5,7,10,14,16,18	4,6,8,13,15,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	3,5,7,10,12,17	4,6,8,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,10,12,16,18	4,6,8,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	3,5,7,10,12,17,18	4,6,8,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,10,12,16	4,6,8,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5,7,10,12,14,18	4,6,8,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	3,5,7,10,12,14,16,17	4,6,8,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5,7,10,12,14	4,6,8,15	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	3,5,7,10,12,14,16,17,18	4,6,8,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	3,5,7,10,12,17,18	4,6,8,13,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	3,5,7,10,12,16	4,6,8,13	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,5,7,10,12,17	4,6,8,13,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,5,7,10,12,16,18	4,6,8,13,15,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	3,5,7,10,12,14	4,6,8,13	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	3,5,7,10,12,14,16,17,18	4,6,8,13,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	3,5,7,10,12,14,18	4,6,8,13,15,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	3,5,7,10,12,14,16,17	4,6,8,13,15,17	$2^{-6.5}$

Table 0.508 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	3,5,7,10	4,6,8,11	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	3,5,7,10,16,17,18	4,6,8,11,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	3,5,7,10,18	4,6,8,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	3,5,7,10,16,17	4,6,8,11,15,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	3,5,7,10,14,17,18	4,6,8,11,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	3,5,7,10,14,16	4,6,8,11	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	3,5,7,10,14,17	4,6,8,11,15,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	3,5,7,10,14,16,18	4,6,8,11,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	3,5,7,10,18	4,6,8,11,13,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	3,5,7,10,16,17	4,6,8,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	3,5,7,10	4,6,8,11,13,15	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	3,5,7,10,16,17,18	4,6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	3,5,7,10,14,17	4,6,8,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,7,10,14,16,18	4,6,8,11,13,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	3,5,7,10,14,17,18	4,6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,7,10,14,16	4,6,8,11,13,15	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	3,5,7,10,12,17,18	4,6,8,11,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	3,5,7,10,12,16	4,6,8,11	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	3,5,7,10,12,17	4,6,8,11,15,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	3,5,7,10,12,16,18	4,6,8,11,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	3,5,7,10,12,14	4,6,8,11	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	3,5,7,10,12,14,16,17,18	4,6,8,11,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	3,5,7,10,12,14,18	4,6,8,11,15,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	3,5,7,10,12,14,16,17	4,6,8,11,15,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	3,5,7,10,12,17	4,6,8,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,7,10,12,16,18	4,6,8,11,13,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	3,5,7,10,12,17,18	4,6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	3,5,7,10,12,16	4,6,8,11,13,15	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	3,5,7,10,12,14,18	4,6,8,11,13,18	2^{-34}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	3,5,7,10,12,14,16,17	4,6,8,11,13,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	3,5,7,10,12,14	4,6,8,11,13,15	2^{-34}
$(0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	3,5,7,10,12,14,16,17,18	4,6,8,11,13,15,17,18	$2^{-17.5}$

Table 0.509 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	3,5,7,17,18	4,6,8,9,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	3,5,7,16	4,6,8,9	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	3,5,7,17	4,6,8,9,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	3,5,7,16,18	4,6,8,9,15,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	3,5,7,14	4,6,8,9	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	3,5,7,14,16,17,18	4,6,8,9,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	3,5,7,14,18	4,6,8,9,15,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	3,5,7,14,16,17	4,6,8,9,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	3,5,7,17	4,6,8,9,13,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	3,5,7,16,18	4,6,8,9,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	3,5,7,17,18	4,6,8,9,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	3,5,7,16	4,6,8,9,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	3,5,7,14,18	4,6,8,9,13,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	3,5,7,14,16,17	4,6,8,9,13,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	3,5,7,14	4,6,8,9,13,15	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	3,5,7,14,16,17,18	4,6,8,9,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	3,5,7,12	4,6,8,9	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	3,5,7,12,16,17,18	4,6,8,9,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	3,5,7,12,18	4,6,8,9,15,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	3,5,7,12,16,17	4,6,8,9,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	3,5,7,12,14,17,18	4,6,8,9,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	3,5,7,12,14,16	4,6,8,9	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	3,5,7,12,14,17	4,6,8,9,15,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	3,5,7,12,14,16,18	4,6,8,9,15,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	3,5,7,12,18	4,6,8,9,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	3,5,7,12,16,17	4,6,8,9,13,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	3,5,7,12	4,6,8,9,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	3,5,7,12,16,17,18	4,6,8,9,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	3,5,7,12,14,17	4,6,8,9,13,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	3,5,7,12,14,16,18	4,6,8,9,13,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	3,5,7,12,14,17,18	4,6,8,9,13,15,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	3,5,7,12,14,16	4,6,8,9,13,15	$2^{-6.5}$

Table 0.510 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	3,5,7,17	4,6,8,9,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	3,5,7,16,18	4,6,8,9,11,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	3,5,7,17,18	4,6,8,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	3,5,7,16	4,6,8,9,11,15	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	3,5,7,14,18	4,6,8,9,11,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	3,5,7,14,16,17	4,6,8,9,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	3,5,7,14	4,6,8,9,11,15	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	3,5,7,14,16,17,18	4,6,8,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	3,5,7,17,18	4,6,8,9,11,13,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	3,5,7,16	4,6,8,9,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	3,5,7,17	4,6,8,9,11,13,15,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	3,5,7,16,18	4,6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	3,5,7,14	4,6,8,9,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	3,5,7,14,16,17,18	4,6,8,9,11,13,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	3,5,7,14,18	4,6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	3,5,7,14,16,17	4,6,8,9,11,13,15,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	3,5,7,12,18	4,6,8,9,11,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	3,5,7,12,16,17	4,6,8,9,11,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	3,5,7,12	4,6,8,9,11,15	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	3,5,7,12,16,17,18	4,6,8,9,11,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	3,5,7,12,14,17	4,6,8,9,11,17	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	3,5,7,12,14,16,18	4,6,8,9,11,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	3,5,7,12,14,17,18	4,6,8,9,11,15,17,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	3,5,7,12,14,16	4,6,8,9,11,15	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,7,12	4,6,8,9,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	3,5,7,12,16,17,18	4,6,8,9,11,13,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,7,12,18	4,6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	3,5,7,12,16,17	4,6,8,9,11,13,15,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	3,5,7,12,14,17,18	4,6,8,9,11,13,17,18	2^{-34}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	3,5,7,12,14,16	4,6,8,9,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	3,5,7,12,14,17	4,6,8,9,11,13,15,17	2^{-34}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	3,5,7,12,14,16,18	4,6,8,9,11,13,15,18	$2^{-17.5}$

Table 0.511 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	3,5,7,10	4,6,8,9	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	3,5,7,10,16,17,18	4,6,8,9,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	3,5,7,10,18	4,6,8,9,15,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	3,5,7,10,16,17	4,6,8,9,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	3,5,7,10,14,17,18	4,6,8,9,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	3,5,7,10,14,16	4,6,8,9	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	3,5,7,10,14,17	4,6,8,9,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	3,5,7,10,14,16,18	4,6,8,9,15,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	3,5,7,10,18	4,6,8,9,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	3,5,7,10,16,17	4,6,8,9,13,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	3,5,7,10	4,6,8,9,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	3,5,7,10,16,17,18	4,6,8,9,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	3,5,7,10,14,17	4,6,8,9,13,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	3,5,7,10,14,16,18	4,6,8,9,13,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	3,5,7,10,14,17,18	4,6,8,9,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	3,5,7,10,14,16	4,6,8,9,13,15	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	3,5,7,10,12,17,18	4,6,8,9,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	3,5,7,10,12,16	4,6,8,9	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	3,5,7,10,12,17	4,6,8,9,15,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	3,5,7,10,12,16,18	4,6,8,9,15,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	3,5,7,10,12,14	4,6,8,9	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	3,5,7,10,12,14,16,17,18	4,6,8,9,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	3,5,7,10,12,14,18	4,6,8,9,15,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	3,5,7,10,12,14,16,17	4,6,8,9,15,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	3,5,7,10,12,17	4,6,8,9,13,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	3,5,7,10,12,16,18	4,6,8,9,13,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	3,5,7,10,12,17,18	4,6,8,9,13,15,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	3,5,7,10,12,16	4,6,8,9,13,15	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	3,5,7,10,12,14,18	4,6,8,9,13,18	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	3,5,7,10,12,14,16,17	4,6,8,9,13,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	3,5,7,10,12,14	4,6,8,9,13,15	$2^{-28.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	3,5,7,10,12,14,16,17,18	4,6,8,9,13,15,17,18	2^{-12}

Table 0.512 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	3,5,7,10,18	4,6,8,9,11,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	3,5,7,10,16,17	4,6,8,9,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	3,5,7,10	4,6,8,9,11,15	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	3,5,7,10,16,17,18	4,6,8,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	3,5,7,10,14,17	4,6,8,9,11,17	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	3,5,7,10,14,16,18	4,6,8,9,11,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	3,5,7,10,14,17,18	4,6,8,9,11,15,17,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	3,5,7,10,14,16	4,6,8,9,11,15	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	3,5,7,10	4,6,8,9,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	3,5,7,10,16,17,18	4,6,8,9,11,13,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	3,5,7,10,18	4,6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	3,5,7,10,16,17	4,6,8,9,11,13,15,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	3,5,7,10,14,17,18	4,6,8,9,11,13,17,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	3,5,7,10,14,16	4,6,8,9,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	3,5,7,10,14,17	4,6,8,9,11,13,15,17	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	3,5,7,10,14,16,18	4,6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	3,5,7,10,12,17	4,6,8,9,11,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	3,5,7,10,12,16,18	4,6,8,9,11,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	3,5,7,10,12,17,18	4,6,8,9,11,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	3,5,7,10,12,16	4,6,8,9,11,15	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	3,5,7,10,12,14,18	4,6,8,9,11,18	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	3,5,7,10,12,14,16,17	4,6,8,9,11,17	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	3,5,7,10,12,14	4,6,8,9,11,15	2^{-23}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	3,5,7,10,12,14,16,17,18	4,6,8,9,11,15,17,18	$2^{-6.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	3,5,7,10,12,17,18	4,6,8,9,11,13,17,18	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,7,10,12,16	4,6,8,9,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	3,5,7,10,12,17	4,6,8,9,11,13,15,17	2^{-12}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,7,10,12,16,18	4,6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	3,5,7,10,12,14	4,6,8,9,11,13	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	3,5,7,10,12,14,16,17,18	4,6,8,9,11,13,17,18	2^{-1}
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	3,5,7,10,12,14,18	4,6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,5,7,10,12,14,16,17	4,6,8,9,11,13,15,17	2^{-1}

Table 0.513 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	17,18	2,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	16	2	2^{-34}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	17	2,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	16,18	2,15,18	2^{-34}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	14	2	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	14,16,17,18	2,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	14,18	2,15,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	14,16,17	2,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	17	2,13,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	16,18	2,13,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	17,18	2,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	16	2,13,15	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	14,18	2,13,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	14,16,17	2,13,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	14	2,13,15	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	14,16,17,18	2,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	12	2	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	12,16,17,18	2,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	12,18	2,15,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	12,16,17	2,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	12,14,17,18	2,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	12,14,16	2	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	12,14,17	2,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	12,14,16,18	2,15,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	12,18	2,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	12,16,17	2,13,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	12	2,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	12,16,17,18	2,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	12,14,17	2,13,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	12,14,16,18	2,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	12,14,17,18	2,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	12,14,16	2,13,15	$2^{-17.5}$

Table 0.514 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	17	2,11,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	16,18	2,11,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	17,18	2,11,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	16	2,11,15	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	14,18	2,11,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	14,16,17	2,11,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	14	2,11,15	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	14,16,17,18	2,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	17,18	2,11,13,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	16	2,11,13	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	17	2,11,13,15,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	16,18	2,11,13,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	14	2,11,13	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	14,16,17,18	2,11,13,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	14,18	2,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	14,16,17	2,11,13,15,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	12,18	2,11,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	12,16,17	2,11,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	12	2,11,15	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	12,16,17,18	2,11,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	12,14,17	2,11,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	12,14,16,18	2,11,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	12,14,17,18	2,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	12,14,16	2,11,15	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	12	2,11,13	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	12,16,17,18	2,11,13,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	12,18	2,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	12,16,17	2,11,13,15,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	12,14,17,18	2,11,13,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	12,14,16	2,11,13	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	12,14,17	2,11,13,15,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	12,14,16,18	2,11,13,15,18	$2^{-28.5}$

Table 0.515 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	10	2	2^{-1}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	10,16,17,18	2,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	10,18	2,15,18	2^{-1}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	10,16,17	2,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	10,14,17,18	2,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	10,14,16	2	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	10,14,17	2,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	10,14,16,18	2,15,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	10,18	2,13,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	10,16,17	2,13,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	10	2,13,15	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	10,16,17,18	2,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	10,14,17	2,13,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	10,14,16,18	2,13,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	10,14,17,18	2,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	10,14,16	2,13,15	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	10,12,17,18	2,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	10,12,16	2	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	10,12,17	2,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	10,12,16,18	2,15,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	10,12,14	2	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	10,12,14,16,17,18	2,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	10,12,14,18	2,15,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	10,12,14,16,17	2,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	10,12,17	2,13,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	10,12,16,18	2,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	10,12,17,18	2,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	10,12,16	2,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	10,12,14,18	2,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	10,12,14,16,17	2,13,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	10,12,14	2,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	10,12,14,16,17,18	2,13,15,17,18	2^{-23}

Table 0.516 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	10,18	2,11,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	10,16,17	2,11,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	10	2,11,15	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	10,16,17,18	2,11,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	10,14,17	2,11,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	10,14,16,18	2,11,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	10,14,17,18	2,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	10,14,16	2,11,15	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	10	2,11,13	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	10,16,17,18	2,11,13,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	10,18	2,11,13,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	10,16,17	2,11,13,15,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	10,14,17,18	2,11,13,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	10,14,16	2,11,13	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	10,14,17	2,11,13,15,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	10,14,16,18	2,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	10,12,17	2,11,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	10,12,16,18	2,11,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	10,12,17,18	2,11,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	10,12,16	2,11,15	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	10,12,14,18	2,11,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	10,12,14,16,17	2,11,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	10,12,14	2,11,15	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	10,12,14,16,17,18	2,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	10,12,17,18	2,11,13,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	10,12,16	2,11,13	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	10,12,17	2,11,13,15,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	10,12,16,18	2,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	10,12,14	2,11,13	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	10,12,14,16,17,18	2,11,13,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	10,12,14,18	2,11,13,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	10,12,14,16,17	2,11,13,15,17	2^{-12}

Table 0.517 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	17	2,9,17	2^{-1}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	16,18	2,9,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	17,18	2,9,15,17,18	2^{-1}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	16	2,9,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	14,18	2,9,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	14,16,17	2,9,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	14	2,9,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	14,16,17,18	2,9,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	17,18	2,9,13,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	16	2,9,13	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	17	2,9,13,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	16,18	2,9,13,15,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	14	2,9,13	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	14,16,17,18	2,9,13,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	14,18	2,9,13,15,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	14,16,17	2,9,13,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	12,18	2,9,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	12,16,17	2,9,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	12	2,9,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	12,16,17,18	2,9,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	12,14,17	2,9,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	12,14,16,18	2,9,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	12,14,17,18	2,9,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	12,14,16	2,9,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	12	2,9,13	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	12,16,17,18	2,9,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	12,18	2,9,13,15,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	12,16,17	2,9,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	12,14,17,18	2,9,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	12,14,16	2,9,13	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	12,14,17	2,9,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	12,14,16,18	2,9,13,15,18	2^{-23}

Table 0.518 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	17,18	2,9,11,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	16	2,9,11	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	17	2,9,11,15,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	16,18	2,9,11,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	14	2,9,11	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	14,16,17,18	2,9,11,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	14,18	2,9,11,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	14,16,17	2,9,11,15,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	17	2,9,11,13,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	16,18	2,9,11,13,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	17,18	2,9,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	16	2,9,11,13,15	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	14,18	2,9,11,13,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	14,16,17	2,9,11,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	14	2,9,11,13,15	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	14,16,17,18	2,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	12	2,9,11	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	12,16,17,18	2,9,11,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	12,18	2,9,11,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	12,16,17	2,9,11,15,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	12,14,17,18	2,9,11,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	12,14,16	2,9,11	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	12,14,17	2,9,11,15,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	12,14,16,18	2,9,11,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	12,18	2,9,11,13,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	12,16,17	2,9,11,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	12	2,9,11,13,15	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	12,16,17,18	2,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	12,14,17	2,9,11,13,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	12,14,16,18	2,9,11,13,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	12,14,17,18	2,9,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	12,14,16	2,9,11,13,15	2^{-12}

Table 0.519 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	10,18	2,9,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	10,16,17	2,9,17	2^{-34}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	10	2,9,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	10,16,17,18	2,9,15,17,18	2^{-34}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	10,14,17	2,9,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	10,14,16,18	2,9,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	10,14,17,18	2,9,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	10,14,16	2,9,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	10	2,9,13	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	10,16,17,18	2,9,13,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	10,18	2,9,13,15,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	10,16,17	2,9,13,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	10,14,17,18	2,9,13,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	10,14,16	2,9,13	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	10,14,17	2,9,13,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	10,14,16,18	2,9,13,15,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	10,12,17	2,9,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	10,12,16,18	2,9,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	10,12,17,18	2,9,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	10,12,16	2,9,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	10,12,14,18	2,9,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	10,12,14,16,17	2,9,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	10,12,14	2,9,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	10,12,14,16,17,18	2,9,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	10,12,17,18	2,9,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	10,12,16	2,9,13	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	10,12,17	2,9,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	10,12,16,18	2,9,13,15,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	10,12,14	2,9,13	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	10,12,14,16,17,18	2,9,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	10,12,14,18	2,9,13,15,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	10,12,14,16,17	2,9,13,15,17	$2^{-17.5}$

Table 0.520 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	10	2,9,11	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	10,16,17,18	2,9,11,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	10,18	2,9,11,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	10,16,17	2,9,11,15,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	10,14,17,18	2,9,11,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	10,14,16	2,9,11	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	10,14,17	2,9,11,15,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	10,14,16,18	2,9,11,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	10,18	2,9,11,13,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	10,16,17	2,9,11,13,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	10	2,9,11,13,15	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	10,16,17,18	2,9,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	10,14,17	2,9,11,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	10,14,16,18	2,9,11,13,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	10,14,17,18	2,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	10,14,16	2,9,11,13,15	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	10,12,17,18	2,9,11,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	10,12,16	2,9,11	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	10,12,17	2,9,11,15,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	10,12,16,18	2,9,11,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	10,12,14	2,9,11	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	10,12,14,16,17,18	2,9,11,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	10,12,14,18	2,9,11,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	10,12,14,16,17	2,9,11,15,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	10,12,17	2,9,11,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	10,12,16,18	2,9,11,13,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	10,12,14,18	2,9,11,13,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	10,12,14,16,17	2,9,11,13,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	10,12,14	2,9,11,13,15	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	10,12,14,16,17,18	2,9,11,13,15,17,18	$2^{-28.5}$

Table 0.521 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	—	2,8	2^{-34}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	16,17,18	2,8,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	18	2,8,15,18	2^{-34}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	16,17	2,8,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	14,17,18	2,8,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	14,16	2,8	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	14,17	2,8,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	14,16,18	2,8,15,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	18	2,8,13,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	16,17	2,8,13,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	—	2,8,13,15	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	16,17,18	2,8,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	14,17	2,8,13,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	14,16,18	2,8,13,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	14,17,18	2,8,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	14,16	2,8,13,15	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	12,17,18	2,8,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	12,16	2,8	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	12,17	2,8,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	12,16,18	2,8,15,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	12,14	2,8	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	12,14,16,17,18	2,8,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	12,14,18	2,8,15,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	12,14,16,17	2,8,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	12,17	2,8,13,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	12,16,18	2,8,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	12,17,18	2,8,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	12,16	2,8,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	12,14,18	2,8,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	12,14,16,17	2,8,13,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	12,14	2,8,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	12,14,16,17,18	2,8,13,15,17,18	2^{-12}

Table 0.522 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	18	2,8,11,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	16,17	2,8,11,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	—	2,8,11,15	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	16,17,18	2,8,11,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	14,17	2,8,11,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	14,16,18	2,8,11,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	14,17,18	2,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	14,16	2,8,11,15	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	—	2,8,11,13	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	16,17,18	2,8,11,13,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	18	2,8,11,13,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	16,17	2,8,11,13,15,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	14,17,18	2,8,11,13,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	14,16	2,8,11,13	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	14,17	2,8,11,13,15,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	14,16,18	2,8,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	12,17	2,8,11,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	12,16,18	2,8,11,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	12,17,18	2,8,11,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	12,16	2,8,11,15	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	12,14,18	2,8,11,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	12,14,16,17	2,8,11,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	12,14	2,8,11,15	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	12,14,16,17,18	2,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	12,17,18	2,8,11,13,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	12,16	2,8,11,13	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	12,17	2,8,11,13,15,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	12,16,18	2,8,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	12,14	2,8,11,13	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	12,14,16,17,18	2,8,11,13,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	12,14,18	2,8,11,13,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	12,14,16,17	2,8,11,13,15,17	2^{-23}

Table 0.523 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	10,17,18	2,8,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	10,16	2,8	2^{-1}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	10,17	2,8,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	10,16,18	2,8,15,18	2^{-1}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	10,14	2,8	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	10,14,16,17,18	2,8,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	10,14,18	2,8,15,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	10,14,16,17	2,8,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	10,17	2,8,13,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	10,16,18	2,8,13,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	10,17,18	2,8,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	10,16	2,8,13,15	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	10,14,18	2,8,13,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	10,14,16,17	2,8,13,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	10,14	2,8,13,15	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	10,14,16,17,18	2,8,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	10,12	2,8	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	10,12,16,17,18	2,8,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	10,12,18	2,8,15,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	10,12,16,17	2,8,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	10,12,14,17,18	2,8,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	10,12,14,16	2,8	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	10,12,14,17	2,8,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	10,12,14,16,18	2,8,15,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	10,12,18	2,8,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	10,12,16,17	2,8,13,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	10,12	2,8,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	10,12,16,17,18	2,8,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	10,12,14,17	2,8,13,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	10,12,14,16,18	2,8,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	10,12,14,17,18	2,8,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	10,12,14,16	2,8,13,15	$2^{-17.5}$

Table 0.524 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	10,17	2,8,11,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	10,16,18	2,8,11,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	10,17,18	2,8,11,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	10,16	2,8,11,15	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	10,14,18	2,8,11,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	10,14,16,17	2,8,11,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	10,14	2,8,11,15	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	10,14,16,17,18	2,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	10,17,18	2,8,11,13,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	10,16	2,8,11,13	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	10,17	2,8,11,13,15,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	10,16,18	2,8,11,13,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	10,14	2,8,11,13	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	10,14,16,17,18	2,8,11,13,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	10,14,18	2,8,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	10,14,16,17	2,8,11,13,15,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	10,12,18	2,8,11,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	10,12,16,17	2,8,11,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	10,12	2,8,11,15	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	10,12,16,17,18	2,8,11,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	10,12,14,17	2,8,11,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	10,12,14,16,18	2,8,11,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	10,12,14,17,18	2,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	10,12,14,16	2,8,11,15	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	10,12	2,8,11,13	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	10,12,16,17,18	2,8,11,13,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	10,12,18	2,8,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	10,12,16,17	2,8,11,13,15,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	10,12,14,17,18	2,8,11,13,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	10,12,14,16	2,8,11,13	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	10,12,14,17	2,8,11,13,15,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	10,12,14,16,18	2,8,11,13,15,18	$2^{-6.5}$

Table 0.525 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	18	2,8,9,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	16,17	2,8,9,17	2^{-1}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	—	2,8,9,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	16,17,18	2,8,9,15,17,18	2^{-1}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	14,17	2,8,9,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	14,16,18	2,8,9,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	14,17,18	2,8,9,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	14,16	2,8,9,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	—	2,8,9,13	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	16,17,18	2,8,9,13,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	18	2,8,9,13,15,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	16,17	2,8,9,13,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	14,17,18	2,8,9,13,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	14,16	2,8,9,13	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	14,17	2,8,9,13,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	14,16,18	2,8,9,13,15,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	12,17	2,8,9,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	12,16,18	2,8,9,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	12,17,18	2,8,9,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	12,16	2,8,9,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	12,14,18	2,8,9,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	12,14,16,17	2,8,9,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	12,14	2,8,9,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	12,14,16,17,18	2,8,9,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	12,17,18	2,8,9,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	12,16	2,8,9,13	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	12,17	2,8,9,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	12,16,18	2,8,9,13,15,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	12,14	2,8,9,13	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	12,14,16,17,18	2,8,9,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	12,14,18	2,8,9,13,15,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	12,14,16,17	2,8,9,13,15,17	$2^{-17.5}$

Table 0.526 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	—	2,8,9,11	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	16,17,18	2,8,9,11,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	18	2,8,9,11,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	16,17	2,8,9,11,15,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	14,17,18	2,8,9,11,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	14,16	2,8,9,11	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	14,17	2,8,9,11,15,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	14,16,18	2,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	18	2,8,9,11,13,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	16,17	2,8,9,11,13,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	—	2,8,9,11,13,15	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	16,17,18	2,8,9,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	14,17	2,8,9,11,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	14,16,18	2,8,9,11,13,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	14,17,18	2,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	14,16	2,8,9,11,13,15	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	12,17,18	2,8,9,11,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	12,16	2,8,9,11	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	12,17	2,8,9,11,15,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	12,16,18	2,8,9,11,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	12,14	2,8,9,11	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	12,14,16,17,18	2,8,9,11,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	12,14,18	2,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	12,14,16,17	2,8,9,11,15,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	12,17	2,8,9,11,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	12,16,18	2,8,9,11,13,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	12,17,18	2,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	12,16	2,8,9,11,13,15	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	12,14,18	2,8,9,11,13,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	12,14,16,17	2,8,9,11,13,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	12,14	2,8,9,11,13,15	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	12,14,16,17,18	2,8,9,11,13,15,17,18	$2^{-6.5}$

Table 0.527 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	10,17	2,8,9,17	2^{-34}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	10,16,18	2,8,9,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	10,17,18	2,8,9,15,17,18	2^{-34}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	10,16	2,8,9,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	10,14,18	2,8,9,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	10,14,16,17	2,8,9,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	10,14	2,8,9,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	10,14,16,17,18	2,8,9,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	10,17,18	2,8,9,13,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	10,16	2,8,9,13	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	10,17	2,8,9,13,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	10,16,18	2,8,9,13,15,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	10,14	2,8,9,13	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	10,14,16,17,18	2,8,9,13,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	10,14,18	2,8,9,13,15,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	10,14,16,17	2,8,9,13,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	10,12,18	2,8,9,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	10,12,16,17	2,8,9,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	10,12	2,8,9,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	10,12,16,17,18	2,8,9,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	10,12,14,17	2,8,9,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	10,12,14,16,18	2,8,9,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	10,12,14,17,18	2,8,9,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	10,12,14,16	2,8,9,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	10,12	2,8,9,13	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	10,12,16,17,18	2,8,9,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	10,12,18	2,8,9,13,15,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	10,12,16,17	2,8,9,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	10,12,14,17,18	2,8,9,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	10,12,14,16	2,8,9,13	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	10,12,14,17	2,8,9,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	10,12,14,16,18	2,8,9,13,15,18	2^{-12}

Table 0.528 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	10,17,18	2,8,9,11,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	10,16	2,8,9,11	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	10,17	2,8,9,11,15,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	10,16,18	2,8,9,11,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	10,14	2,8,9,11	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	10,14,16,17,18	2,8,9,11,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	10,14,18	2,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	10,14,16,17	2,8,9,11,15,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	10,17	2,8,9,11,13,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	10,16,18	2,8,9,11,13,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	10,17,18	2,8,9,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	10,16	2,8,9,11,13,15	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	10,14,18	2,8,9,11,13,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	10,14,16,17	2,8,9,11,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	10,14	2,8,9,11,13,15	2^{-12}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	10,14,16,17,18	2,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	10,12	2,8,9,11	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	10,12,16,17,18	2,8,9,11,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	10,12,18	2,8,9,11,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	10,12,16,17	2,8,9,11,15,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	10,12,14,17,18	2,8,9,11,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	10,12,14,16	2,8,9,11	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	10,12,14,17	2,8,9,11,15,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	10,12,14,16,18	2,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	10,12,18	2,8,9,11,13,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	10,12,16,17	2,8,9,11,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	10,12	2,8,9,11,13,15	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	10,12,16,17,18	2,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	10,12,14,17	2,8,9,11,13,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	10,12,14,16,18	2,8,9,11,13,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	10,12,14,17,18	2,8,9,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	10,12,14,16	2,8,9,11,13,15	2^{-23}

Table 0.529 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	7,17	2,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	7,16,18	2,18	2^{-34}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	7,17,18	2,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	7,16	2,15	2^{-34}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	7,14,18	2,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	7,14,16,17	2,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	7,14	2,15	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	7,14,16,17,18	2,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	7,17,18	2,13,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	7,16	2,13	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	7,17	2,13,15,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	7,16,18	2,13,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	7,14	2,13	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	7,14,16,17,18	2,13,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	7,14,18	2,13,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	7,14,16,17	2,13,15,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	7,12,18	2,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	7,12,16,17	2,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	7,12	2,15	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	7,12,16,17,18	2,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	7,12,14,17	2,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	7,12,14,16,18	2,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	7,12,14,17,18	2,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	7,12,14,16	2,15	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	7,12	2,13	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	7,12,16,17,18	2,13,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	7,12,18	2,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	7,12,16,17	2,13,15,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	7,12,14,17,18	2,13,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	7,12,14,16	2,13	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	7,12,14,17	2,13,15,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	7,12,14,16,18	2,13,15,18	$2^{-17.5}$

Table 0.530 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	7,17,18	2,11,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	7,16	2,11	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	7,17	2,11,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	7,16,18	2,11,15,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	7,14	2,11	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	7,14,16,17,18	2,11,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	7,14,18	2,11,15,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	7,14,16,17	2,11,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	7,17	2,11,13,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	7,16,18	2,11,13,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	7,17,18	2,11,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	7,16	2,11,13,15	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	7,14,18	2,11,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	7,14,16,17	2,11,13,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	7,14	2,11,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	7,14,16,17,18	2,11,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	7,12	2,11	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	7,12,16,17,18	2,11,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	7,12,18	2,11,15,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	7,12,16,17	2,11,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	7,12,14,17,18	2,11,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	7,12,14,16	2,11	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	7,12,14,17	2,11,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	7,12,14,16,18	2,11,15,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	7,12,18	2,11,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	7,12,16,17	2,11,13,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	7,12	2,11,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	7,12,16,17,18	2,11,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	7,12,14,17	2,11,13,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	7,12,14,16,18	2,11,13,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	7,12,14,17,18	2,11,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	7,12,14,16	2,11,13,15	$2^{-28.5}$

Table 0.531 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	7,10,18	2,18	2^{-1}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	7,10,16,17	2,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	7,10	2,15	2^{-1}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	7,10,16,17,18	2,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	7,10,14,17	2,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	7,10,14,16,18	2,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	7,10,14,17,18	2,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	7,10,14,16	2,15	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	7,10	2,13	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	7,10,16,17,18	2,13,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	7,10,18	2,13,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	7,10,16,17	2,13,15,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	7,10,14,17,18	2,13,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	7,10,14,16	2,13	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	7,10,14,17	2,13,15,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	7,10,14,16,18	2,13,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	7,10,12,17	2,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	7,10,12,16,18	2,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	7,10,12,17,18	2,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	7,10,12,16	2,15	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	7,10,12,14,18	2,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	7,10,12,14,16,17	2,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	7,10,12,14	2,15	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	7,10,12,14,16,17,18	2,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	7,10,12,17,18	2,13,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	7,10,12,16	2,13	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	7,10,12,17	2,13,15,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	7,10,12,16,18	2,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	7,10,12,14	2,13	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	7,10,12,14,16,17,18	2,13,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	7,10,12,14,18	2,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	7,10,12,14,16,17	2,13,15,17	2^{-23}

Table 0.532 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	7,10	2,11	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	7,10,16,17,18	2,11,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	7,10,18	2,11,15,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	7,10,16,17	2,11,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	7,10,14,17,18	2,11,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	7,10,14,16	2,11	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	7,10,14,17	2,11,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	7,10,14,16,18	2,11,15,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	7,10,18	2,11,13,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	7,10,16,17	2,11,13,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	7,10	2,11,13,15	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	7,10,16,17,18	2,11,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	7,10,14,17	2,11,13,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	7,10,14,16,18	2,11,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	7,10,14,17,18	2,11,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	7,10,14,16	2,11,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	7,10,12,17,18	2,11,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	7,10,12,16	2,11	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	7,10,12,17	2,11,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	7,10,12,16,18	2,11,15,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	7,10,12,14	2,11	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	7,10,12,14,16,17,18	2,11,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	7,10,12,14,18	2,11,15,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	7,10,12,14,16,17	2,11,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	7,10,12,17	2,11,13,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	7,10,12,16,18	2,11,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	7,10,12,17,18	2,11,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	7,10,12,16	2,11,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	7,10,12,14,18	2,11,13,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	7,10,12,14,16,17	2,11,13,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	7,10,12,14	2,11,13,15	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	7,10,12,14,16,17,18	2,11,13,15,17,18	2^{-12}

Table 0.533 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	7,17,18	2,9,17,18	2^{-1}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	7,16	2,9	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	7,17	2,9,15,17	2^{-1}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	7,16,18	2,9,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	7,14	2,9	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	7,14,16,17,18	2,9,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	7,14,18	2,9,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	7,14,16,17	2,9,15,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	7,17	2,9,13,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	7,16,18	2,9,13,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	7,17,18	2,9,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	7,16	2,9,13,15	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	7,14,18	2,9,13,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	7,14,16,17	2,9,13,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	7,14	2,9,13,15	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	7,14,16,17,18	2,9,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	7,12	2,9	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	7,12,16,17,18	2,9,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	7,12,18	2,9,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	7,12,16,17	2,9,15,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	7,12,14,17,18	2,9,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	7,12,14,16	2,9	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	7,12,14,17	2,9,15,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	7,12,14,16,18	2,9,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	7,12,18	2,9,13,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	7,12,16,17	2,9,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	7,12	2,9,13,15	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	7,12,16,17,18	2,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	7,12,14,17	2,9,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	7,12,14,16,18	2,9,13,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	7,12,14,17,18	2,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	7,12,14,16	2,9,13,15	2^{-23}

Table 0.534 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	7,17	2,9,11,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	7,16,18	2,9,11,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	7,17,18	2,9,11,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	7,16	2,9,11,15	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	7,14,18	2,9,11,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	7,14,16,17	2,9,11,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	7,14	2,9,11,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	7,14,16,17,18	2,9,11,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	7,17,18	2,9,11,13,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	7,16	2,9,11,13	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	7,17	2,9,11,13,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	7,16,18	2,9,11,13,15,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	7,14	2,9,11,13	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	7,14,16,17,18	2,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	7,14,18	2,9,11,13,15,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	7,14,16,17	2,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	7,12,18	2,9,11,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	7,12,16,17	2,9,11,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	7,12	2,9,11,15	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	7,12,16,17,18	2,9,11,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	7,12,14,17	2,9,11,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	7,12,14,16,18	2,9,11,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	7,12,14,17,18	2,9,11,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	7,12,14,16	2,9,11,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	7,12	2,9,11,13	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	7,12,16,17,18	2,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	7,12,18	2,9,11,13,15,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	7,12,16,17	2,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	7,12,14,17,18	2,9,11,13,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	7,12,14,16	2,9,11,13	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	7,12,14,17	2,9,11,13,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	7,12,14,16,18	2,9,11,13,15,18	2^{-12}

Table 0.535 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	7,10	2,9	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	7,10,16,17,18	2,9,17,18	2^{-34}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	7,10,18	2,9,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	7,10,16,17	2,9,15,17	2^{-34}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	7,10,14,17,18	2,9,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	7,10,14,16	2,9	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	7,10,14,17	2,9,15,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	7,10,14,16,18	2,9,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	7,10,18	2,9,13,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	7,10,16,17	2,9,13,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	7,10	2,9,13,15	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	7,10,16,17,18	2,9,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	7,10,14,17	2,9,13,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	7,10,14,16,18	2,9,13,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	7,10,14,17,18	2,9,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	7,10,14,16	2,9,13,15	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	7,10,12,17,18	2,9,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	7,10,12,16	2,9	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	7,10,12,17	2,9,15,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	7,10,12,16,18	2,9,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	7,10,12,14	2,9	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	7,10,12,14,16,17,18	2,9,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	7,10,12,14,18	2,9,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	7,10,12,14,16,17	2,9,15,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	7,10,12,17	2,9,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	7,10,12,16,18	2,9,13,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	7,10,12,17,18	2,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	7,10,12,16	2,9,13,15	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	7,10,12,14,18	2,9,13,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	7,10,12,14,16,17	2,9,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	7,10,12,14	2,9,13,15	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	7,10,12,14,16,17,18	2,9,13,15,17,18	$2^{-17.5}$

Table 0.536 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	7,10,18	2,9,11,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	7,10,16,17	2,9,11,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	7,10	2,9,11,15	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	7,10,16,17,18	2,9,11,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	7,10,14,17	2,9,11,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	7,10,14,16,18	2,9,11,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	7,10,14,17,18	2,9,11,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	7,10,14,16	2,9,11,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	7,10	2,9,11,13	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	7,10,16,17,18	2,9,11,13,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	7,10,18	2,9,11,13,15,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	7,10,16,17	2,9,11,13,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	7,10,14,17,18	2,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	7,10,14,16	2,9,11,13	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	7,10,14,17	2,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	7,10,14,16,18	2,9,11,13,15,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	7,10,12,17	2,9,11,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	7,10,12,16,18	2,9,11,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	7,10,12,17,18	2,9,11,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	7,10,12,16	2,9,11,15	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	7,10,12,14,18	2,9,11,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	7,10,12,14,16,17	2,9,11,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	7,10,12,14	2,9,11,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	7,10,12,14,16,17,18	2,9,11,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	7,10,12,17,18	2,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	7,10,12,16	2,9,11,13	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	7,10,12,17	2,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	7,10,12,16,18	2,9,11,13,15,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	7,10,12,14	2,9,11,13	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	7,10,12,14,16,17,18	2,9,11,13,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	7,10,12,14,18	2,9,11,13,15,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	7,10,12,14,16,17	2,9,11,13,15,17	$2^{-28.5}$

Table 0.537 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	7,18	2,8,18	2^{-34}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	7,16,17	2,8,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	7	2,8,15	2^{-34}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	7,16,17,18	2,8,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	7,14,17	2,8,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	7,14,16,18	2,8,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	7,14,17,18	2,8,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	7,14,16	2,8,15	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	7	2,8,13	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	7,16,17,18	2,8,13,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	7,18	2,8,13,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	7,16,17	2,8,13,15,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	7,14,17,18	2,8,13,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	7,14,16	2,8,13	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	7,14,17	2,8,13,15,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	7,14,16,18	2,8,13,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	7,12,17	2,8,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	7,12,16,18	2,8,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	7,12,17,18	2,8,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	7,12,16	2,8,15	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	7,12,14,18	2,8,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	7,12,14,16,17	2,8,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	7,12,14	2,8,15	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	7,12,14,16,17,18	2,8,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	7,12,17,18	2,8,13,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	7,12,16	2,8,13	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	7,12,17	2,8,13,15,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	7,12,16,18	2,8,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	7,12,14	2,8,13	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	7,12,14,16,17,18	2,8,13,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	7,12,14,18	2,8,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	7,12,14,16,17	2,8,13,15,17	2^{-12}

Table 0.538 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	7	2,8,11	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	7,16,17,18	2,8,11,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	7,18	2,8,11,15,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	7,16,17	2,8,11,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	7,14,17,18	2,8,11,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	7,14,16	2,8,11	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	7,14,17	2,8,11,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	7,14,16,18	2,8,11,15,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	7,18	2,8,11,13,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	7,16,17	2,8,11,13,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	7	2,8,11,13,15	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	7,16,17,18	2,8,11,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	7,14,17	2,8,11,13,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	7,14,16,18	2,8,11,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	7,14,17,18	2,8,11,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	7,14,16	2,8,11,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	7,12,17,18	2,8,11,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	7,12,16	2,8,11	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	7,12,17	2,8,11,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	7,12,16,18	2,8,11,15,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	7,12,14	2,8,11	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	7,12,14,16,17,18	2,8,11,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	7,12,14,18	2,8,11,15,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	7,12,14,16,17	2,8,11,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	7,12,17	2,8,11,13,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	7,12,16,18	2,8,11,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	7,12,17,18	2,8,11,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	7,12,16	2,8,11,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	7,12,14,18	2,8,11,13,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	7,12,14,16,17	2,8,11,13,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	7,12,14	2,8,11,13,15	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	7,12,14,16,17,18	2,8,11,13,15,17,18	2^{-23}

Table 0.539 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(2)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	7,10,17	2,8,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	7,10,16,18	2,8,18	2^{-1}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	7,10,17,18	2,8,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	7,10,16	2,8,15	2^{-1}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	7,10,14,18	2,8,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	7,10,14,16,17	2,8,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	7,10,14	2,8,15	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	7,10,14,16,17,18	2,8,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	7,10,17,18	2,8,13,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	7,10,16	2,8,13	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	7,10,17	2,8,13,15,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	7,10,16,18	2,8,13,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	7,10,14	2,8,13	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	7,10,14,16,17,18	2,8,13,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	7,10,14,18	2,8,13,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	7,10,14,16,17	2,8,13,15,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	7,10,12,18	2,8,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	7,10,12,16,17	2,8,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	7,10,12	2,8,15	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	7,10,12,16,17,18	2,8,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	7,10,12,14,17	2,8,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	7,10,12,14,16,18	2,8,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	7,10,12,14,17,18	2,8,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	7,10,12,14,16	2,8,15	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	7,10,12	2,8,13	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	7,10,12,16,17,18	2,8,13,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	7,10,12,18	2,8,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	7,10,12,16,17	2,8,13,15,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	7,10,12,14,17,18	2,8,13,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	7,10,12,14,16	2,8,13	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	7,10,12,14,17	2,8,13,15,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	7,10,12,14,16,18	2,8,13,15,18	$2^{-17.5}$

Table 0.540 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	7,10,17,18	2,8,11,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	7,10,16	2,8,11	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	7,10,17	2,8,11,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	7,10,16,18	2,8,11,15,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	7,10,14	2,8,11	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	7,10,14,16,17,18	2,8,11,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	7,10,14,18	2,8,11,15,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	7,10,14,16,17	2,8,11,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	7,10,17	2,8,11,13,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	7,10,16,18	2,8,11,13,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	7,10,17,18	2,8,11,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	7,10,16	2,8,11,13,15	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	7,10,14,18	2,8,11,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	7,10,14,16,17	2,8,11,13,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	7,10,14	2,8,11,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	7,10,14,16,17,18	2,8,11,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	7,10,12	2,8,11	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	7,10,12,16,17,18	2,8,11,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	7,10,12,18	2,8,11,15,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	7,10,12,16,17	2,8,11,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	7,10,12,14,17,18	2,8,11,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	7,10,12,14,16	2,8,11	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	7,10,12,14,17	2,8,11,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	7,10,12,14,16,18	2,8,11,15,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	7,10,12,18	2,8,11,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	7,10,12,16,17	2,8,11,13,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	7,10,12	2,8,11,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	7,10,12,16,17,18	2,8,11,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	7,10,12,14,17	2,8,11,13,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	7,10,12,14,16,18	2,8,11,13,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	7,10,12,14,17,18	2,8,11,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	7,10,12,14,16	2,8,11,13,15	$2^{-6.5}$

Table 0.541 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	7	2,8,9	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	7,16,17,18	2,8,9,17,18	2^{-1}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	7,18	2,8,9,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	7,16,17	2,8,9,15,17	2^{-1}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	7,14,17,18	2,8,9,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	7,14,16	2,8,9	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	7,14,17	2,8,9,15,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	7,14,16,18	2,8,9,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	7,18	2,8,9,13,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	7,16,17	2,8,9,13,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	7	2,8,9,13,15	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	7,16,17,18	2,8,9,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	7,14,17	2,8,9,13,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	7,14,16,18	2,8,9,13,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	7,14,17,18	2,8,9,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	7,14,16	2,8,9,13,15	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	7,12,17,18	2,8,9,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	7,12,16	2,8,9	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	7,12,17	2,8,9,15,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	7,12,16,18	2,8,9,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	7,12,14	2,8,9	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	7,12,14,16,17,18	2,8,9,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	7,12,14,18	2,8,9,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	7,12,14,16,17	2,8,9,15,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	7,12,17	2,8,9,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	7,12,17,18	2,8,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	7,12,16	2,8,9,13,15	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	7,12,14,18	2,8,9,13,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	7,12,14,16,17	2,8,9,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	7,12,14	2,8,9,13,15	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	7,12,14,16,17,18	2,8,9,13,15,17,18	$2^{-17.5}$

Table 0.542 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	7,18	2,8,9,11,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	7,16,17	2,8,9,11,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	7	2,8,9,11,15	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	7,16,17,18	2,8,9,11,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	7,14,17	2,8,9,11,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	7,14,16,18	2,8,9,11,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	7,14,17,18	2,8,9,11,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	7,14,16	2,8,9,11,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	7	2,8,9,11,13	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	7,16,17,18	2,8,9,11,13,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	7,18	2,8,9,11,13,15,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	7,16,17	2,8,9,11,13,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	7,14,17,18	2,8,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	7,14,16	2,8,9,11,13	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	7,14,17	2,8,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	7,14,16,18	2,8,9,11,13,15,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	7,12,17	2,8,9,11,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	7,12,16,18	2,8,9,11,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	7,12,17,18	2,8,9,11,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	7,12,16	2,8,9,11,15	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	7,12,14,18	2,8,9,11,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	7,12,14,16,17	2,8,9,11,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	7,12,14	2,8,9,11,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	7,12,14,16,17,18	2,8,9,11,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	7,12,17,18	2,8,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	7,12,16	2,8,9,11,13	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	7,12,17	2,8,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	7,12,16,18	2,8,9,11,13,15,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	7,12,14	2,8,9,11,13	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	7,12,14,16,17,18	2,8,9,11,13,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	7,12,14,18	2,8,9,11,13,15,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	7,12,14,16,17	2,8,9,11,13,15,17	$2^{-6.5}$

Table 0.543 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	7,10,17,18	2,8,9,17,18	2^{-34}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	7,10,16	2,8,9	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	7,10,17	2,8,9,15,17	2^{-34}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	7,10,16,18	2,8,9,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	7,10,14	2,8,9	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	7,10,14,16,17,18	2,8,9,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	7,10,14,18	2,8,9,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	7,10,14,16,17	2,8,9,15,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	7,10,17	2,8,9,13,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	7,10,16,18	2,8,9,13,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	7,10,17,18	2,8,9,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	7,10,16	2,8,9,13,15	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	7,10,14,18	2,8,9,13,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	7,10,14,16,17	2,8,9,13,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	7,10,14	2,8,9,13,15	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	7,10,14,16,17,18	2,8,9,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	7,10,12	2,8,9	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	7,10,12,16,17,18	2,8,9,17,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	7,10,12,18	2,8,9,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	7,10,12,16,17	2,8,9,15,17	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	7,10,12,14,17,18	2,8,9,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	7,10,12,14,16	2,8,9	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	7,10,12,14,17	2,8,9,15,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	7,10,12,14,16,18	2,8,9,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	7,10,12,18	2,8,9,13,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	7,10,12,16,17	2,8,9,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	7,10,12	2,8,9,13,15	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	7,10,12,16,17,18	2,8,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	7,10,12,14,17	2,8,9,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	7,10,12,14,16,18	2,8,9,13,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	7,10,12,14,17,18	2,8,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	7,10,12,14,16	2,8,9,13,15	2^{-12}

Table 0.544 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	7,10,17	2,8,9,11,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	7,10,16,18	2,8,9,11,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	7,10,17,18	2,8,9,11,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	7,10,16	2,8,9,11,15	$2^{-6.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	7,10,14,18	2,8,9,11,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	7,10,14,16,17	2,8,9,11,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	7,10,14	2,8,9,11,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	7,10,14,16,17,18	2,8,9,11,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	7,10,17,18	2,8,9,11,13,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	7,10,16	2,8,9,11,13	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	7,10,17	2,8,9,11,13,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	7,10,16,18	2,8,9,11,13,15,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	7,10,14	2,8,9,11,13	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	7,10,14,16,17,18	2,8,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	7,10,14,18	2,8,9,11,13,15,18	2^{-12}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	7,10,14,16,17	2,8,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	7,10,12,18	2,8,9,11,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	7,10,12,16,17	2,8,9,11,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	7,10,12	2,8,9,11,15	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	7,10,12,16,17,18	2,8,9,11,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	7,10,12,14,17	2,8,9,11,17	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	7,10,12,14,16,18	2,8,9,11,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	7,10,12,14,17,18	2,8,9,11,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	7,10,12,14,16	2,8,9,11,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	7,10,12	2,8,9,11,13	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	7,10,12,16,17,18	2,8,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	7,10,12,18	2,8,9,11,13,15,18	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	7,10,12,16,17	2,8,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	7,10,12,14,17,18	2,8,9,11,13,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	7,10,12,14,16	2,8,9,11,13	2^{-23}
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	7,10,12,14,17	2,8,9,11,13,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	7,10,12,14,16,18	2,8,9,11,13,15,18	2^{-23}

Table 0.545 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	—	2,6	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	16,17,18	2,6,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	18	2,6,15,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	16,17	2,6,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	14,17,18	2,6,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	14,16	2,6	2^{-34}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	14,17	2,6,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	14,16,18	2,6,15,18	2^{-34}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	18	2,6,13,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	16,17	2,6,13,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	—	2,6,13,15	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	16,17,18	2,6,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	14,17	2,6,13,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	14,16,18	2,6,13,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	14,17,18	2,6,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	14,16	2,6,13,15	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	12,17,18	2,6,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	12,16	2,6	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	12,17	2,6,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	12,16,18	2,6,15,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	12,14	2,6	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	12,14,16,17,18	2,6,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	12,14,18	2,6,15,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	12,14,16,17	2,6,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	12,17	2,6,13,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	12,16,18	2,6,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	12,17,18	2,6,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	12,16	2,6,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	12,14,18	2,6,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	12,14,16,17	2,6,13,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	12,14	2,6,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	12,14,16,17,18	2,6,13,15,17,18	2^{-23}

Table 0.546 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	18	2,6,11,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	16,17	2,6,11,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	—	2,6,11,15	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	16,17,18	2,6,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	14,17	2,6,11,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	14,16,18	2,6,11,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	14,17,18	2,6,11,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	14,16	2,6,11,15	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	—	2,6,11,13	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	16,17,18	2,6,11,13,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	18	2,6,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	16,17	2,6,11,13,15,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	14,17,18	2,6,11,13,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	14,16	2,6,11,13	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	14,17	2,6,11,13,15,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	14,16,18	2,6,11,13,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	12,17	2,6,11,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	12,16,18	2,6,11,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	12,17,18	2,6,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	12,16	2,6,11,15	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	12,14,18	2,6,11,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	12,14,16,17	2,6,11,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	12,14	2,6,11,15	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	12,14,16,17,18	2,6,11,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	12,17,18	2,6,11,13,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	12,16	2,6,11,13	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	12,17	2,6,11,13,15,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	12,16,18	2,6,11,13,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	12,14	2,6,11,13	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	12,14,16,17,18	2,6,11,13,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	12,14,18	2,6,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	12,14,16,17	2,6,11,13,15,17	2^{-23}

Table 0.547 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	10,17,18	2,6,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	10,16	2,6	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	10,17	2,6,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	10,16,18	2,6,15,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	10,14	2,6	2^{-1}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	10,14,16,17,18	2,6,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	10,14,18	2,6,15,18	2^{-1}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	10,14,16,17	2,6,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	10,17	2,6,13,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	10,16,18	2,6,13,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	10,17,18	2,6,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	10,16	2,6,13,15	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	10,14,18	2,6,13,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	10,14,16,17	2,6,13,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	10,14	2,6,13,15	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	10,14,16,17,18	2,6,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	10,12	2,6	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	10,12,16,17,18	2,6,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	10,12,18	2,6,15,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	10,12,16,17	2,6,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	10,12,14,17,18	2,6,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	10,12,14,16	2,6	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	10,12,14,17	2,6,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	10,12,14,16,18	2,6,15,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	10,12,18	2,6,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	10,12,16,17	2,6,13,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	10,12	2,6,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	10,12,16,17,18	2,6,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	10,12,14,17	2,6,13,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	10,12,14,16,18	2,6,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	10,12,14,17,18	2,6,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	10,12,14,16	2,6,13,15	$2^{-17.5}$

Table 0.548 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	10,17	2,6,11,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	10,16,18	2,6,11,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	10,17,18	2,6,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	10,16	2,6,11,15	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	10,14,18	2,6,11,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	10,14,16,17	2,6,11,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	10,14	2,6,11,15	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	10,14,16,17,18	2,6,11,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	10,17,18	2,6,11,13,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	10,16	2,6,11,13	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	10,17	2,6,11,13,15,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	10,16,18	2,6,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	10,14	2,6,11,13	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	10,14,16,17,18	2,6,11,13,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	10,14,18	2,6,11,13,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	10,14,16,17	2,6,11,13,15,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	10,12,18	2,6,11,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	10,12,16,17	2,6,11,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	10,12	2,6,11,15	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	10,12,16,17,18	2,6,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	10,12,14,17	2,6,11,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	10,12,14,16,18	2,6,11,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	10,12,14,17,18	2,6,11,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	10,12,14,16	2,6,11,15	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	10,12	2,6,11,13	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	10,12,16,17,18	2,6,11,13,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	10,12,18	2,6,11,13,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	10,12,16,17	2,6,11,13,15,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	10,12,14,17,18	2,6,11,13,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	10,12,14,16	2,6,11,13	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	10,12,14,17	2,6,11,13,15,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	10,12,14,16,18	2,6,11,13,15,18	$2^{-17.5}$

Table 0.549 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	18	2,6,9,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	16,17	2,6,9,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	—	2,6,9,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	16,17,18	2,6,9,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	14,17	2,6,9,17	2^{-1}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	14,16,18	2,6,9,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	14,17,18	2,6,9,15,17,18	2^{-1}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	14,16	2,6,9,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	—	2,6,9,13	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	16,17,18	2,6,9,13,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	18	2,6,9,13,15,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	16,17	2,6,9,13,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	14,17,18	2,6,9,13,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	14,16	2,6,9,13	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	14,17	2,6,9,13,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	14,16,18	2,6,9,13,15,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	12,17	2,6,9,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	12,16,18	2,6,9,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	12,17,18	2,6,9,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	12,16	2,6,9,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	12,14,18	2,6,9,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	12,14,16,17	2,6,9,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	12,14	2,6,9,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	12,14,16,17,18	2,6,9,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	12,17,18	2,6,9,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	12,16	2,6,9,13	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	12,17	2,6,9,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	12,16,18	2,6,9,13,15,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	12,14	2,6,9,13	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	12,14,16,17,18	2,6,9,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	12,14,18	2,6,9,13,15,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	12,14,16,17	2,6,9,13,15,17	$2^{-17.5}$

Table 0.550 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	—	2,6,9,11	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	16,17,18	2,6,9,11,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	18	2,6,9,11,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	16,17	2,6,9,11,15,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	14,17,18	2,6,9,11,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	14,16	2,6,9,11	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	14,17	2,6,9,11,15,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	14,16,18	2,6,9,11,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	18	2,6,9,11,13,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	16,17	2,6,9,11,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	—	2,6,9,11,13,15	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	16,17,18	2,6,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	14,17	2,6,9,11,13,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	14,16,18	2,6,9,11,13,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	14,17,18	2,6,9,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	14,16	2,6,9,11,13,15	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	12,17,18	2,6,9,11,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	12,16	2,6,9,11	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	12,17	2,6,9,11,15,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	12,16,18	2,6,9,11,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	12,14	2,6,9,11	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	12,14,16,17,18	2,6,9,11,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	12,14,18	2,6,9,11,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	12,14,16,17	2,6,9,11,15,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	12,17	2,6,9,11,13,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	12,16,18	2,6,9,11,13,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	12,17,18	2,6,9,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	12,16	2,6,9,11,13,15	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	12,14,18	2,6,9,11,13,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	12,14,16,17	2,6,9,11,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	12,14	2,6,9,11,13,15	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	12,14,16,17,18	2,6,9,11,13,15,17,18	$2^{-17.5}$

Table 0.551 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	10,17	2,6,9,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	10,16,18	2,6,9,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	10,17,18	2,6,9,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	10,16	2,6,9,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	10,14,18	2,6,9,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	10,14,16,17	2,6,9,17	2^{-34}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	10,14	2,6,9,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	10,14,16,17,18	2,6,9,15,17,18	2^{-34}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	10,17,18	2,6,9,13,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	10,16	2,6,9,13	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	10,17	2,6,9,13,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	10,16,18	2,6,9,13,15,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	10,14	2,6,9,13	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	10,14,16,17,18	2,6,9,13,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	10,14,18	2,6,9,13,15,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	10,14,16,17	2,6,9,13,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	10,12,18	2,6,9,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	10,12,16,17	2,6,9,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	10,12	2,6,9,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	10,12,16,17,18	2,6,9,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	10,12,14,17	2,6,9,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	10,12,14,16,18	2,6,9,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	10,12,14,17,18	2,6,9,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	10,12,14,16	2,6,9,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	10,12	2,6,9,13	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	10,12,16,17,18	2,6,9,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	10,12,18	2,6,9,13,15,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	10,12,16,17	2,6,9,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	10,12,14,17,18	2,6,9,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	10,12,14,16	2,6,9,13	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	10,12,14,17	2,6,9,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	10,12,14,16,18	2,6,9,13,15,18	2^{-23}

Table 0.552 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	10,17,18	2,6,9,11,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	10,16	2,6,9,11	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	10,17	2,6,9,11,15,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	10,16,18	2,6,9,11,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	10,14	2,6,9,11	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	10,14,16,17,18	2,6,9,11,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	10,14,18	2,6,9,11,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	10,14,16,17	2,6,9,11,15,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	10,17	2,6,9,11,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	10,16,18	2,6,9,11,13,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	10,17,18	2,6,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	10,16	2,6,9,11,13,15	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	10,14,18	2,6,9,11,13,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	10,14,16,17	2,6,9,11,13,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	10,14	2,6,9,11,13,15	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	10,14,16,17,18	2,6,9,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	10,12	2,6,9,11	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	10,12,16,17,18	2,6,9,11,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	10,12,18	2,6,9,11,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	10,12,16,17	2,6,9,11,15,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	10,12,14,17,18	2,6,9,11,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	10,12,14,16	2,6,9,11	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	10,12,14,17	2,6,9,11,15,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	10,12,14,16,18	2,6,9,11,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	10,12,18	2,6,9,11,13,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	10,12,16,17	2,6,9,11,13,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	10,12	2,6,9,11,13,15	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	10,12,16,17,18	2,6,9,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	10,12,14,17	2,6,9,11,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	10,12,14,16,18	2,6,9,11,13,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	10,12,14,17,18	2,6,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	10,12,14,16	2,6,9,11,13,15	2^{-23}

Table 0.553 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	17,18	2,6,8,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	16	2,6,8	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	17	2,6,8,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	16,18	2,6,8,15,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	14	2,6,8	2^{-34}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	14,16,17,18	2,6,8,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	14,18	2,6,8,15,18	2^{-34}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	14,16,17	2,6,8,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	17	2,6,8,13,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	16,18	2,6,8,13,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	17,18	2,6,8,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	16	2,6,8,13,15	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	14,18	2,6,8,13,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	14,16,17	2,6,8,13,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	14	2,6,8,13,15	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	14,16,17,18	2,6,8,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	12	2,6,8	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	12,16,17,18	2,6,8,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	12,18	2,6,8,15,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	12,16,17	2,6,8,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	12,14,17,18	2,6,8,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	12,14,16	2,6,8	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	12,14,17	2,6,8,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	12,14,16,18	2,6,8,15,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	12,18	2,6,8,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	12,16,17	2,6,8,13,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	12	2,6,8,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	12,16,17,18	2,6,8,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	12,14,17	2,6,8,13,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	12,14,16,18	2,6,8,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	12,14,17,18	2,6,8,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	12,14,16	2,6,8,13,15	$2^{-17.5}$

Table 0.554 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	17	2,6,8,11,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	16,18	2,6,8,11,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	17,18	2,6,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	16	2,6,8,11,15	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	14,18	2,6,8,11,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	14,16,17	2,6,8,11,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	14	2,6,8,11,15	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	14,16,17,18	2,6,8,11,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	17,18	2,6,8,11,13,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	16	2,6,8,11,13	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	17	2,6,8,11,13,15,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	16,18	2,6,8,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	14	2,6,8,11,13	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	14,16,17,18	2,6,8,11,13,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	14,18	2,6,8,11,13,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	14,16,17	2,6,8,11,13,15,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	12,18	2,6,8,11,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	12,16,17	2,6,8,11,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	12	2,6,8,11,15	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	12,16,17,18	2,6,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	12,14,17	2,6,8,11,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	12,14,16,18	2,6,8,11,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	12,14,17,18	2,6,8,11,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	12,14,16	2,6,8,11,15	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	12	2,6,8,11,13	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	12,16,17,18	2,6,8,11,13,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	12,18	2,6,8,11,13,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	12,16,17	2,6,8,11,13,15,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	12,14,17,18	2,6,8,11,13,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	12,14,16	2,6,8,11,13	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	12,14,17	2,6,8,11,13,15,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	12,14,16,18	2,6,8,11,13,15,18	$2^{-17.5}$

Table 0.555 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	10	2,6,8	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	10,16,17,18	2,6,8,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	10,18	2,6,8,15,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	10,16,17	2,6,8,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	10,14,17,18	2,6,8,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	10,14,16	2,6,8	2^{-1}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	10,14,17	2,6,8,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	10,14,16,18	2,6,8,15,18	2^{-1}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	10,18	2,6,8,13,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	10,16,17	2,6,8,13,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	10	2,6,8,13,15	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	10,16,17,18	2,6,8,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	10,14,17	2,6,8,13,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	10,14,16,18	2,6,8,13,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	10,14,17,18	2,6,8,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	10,14,16	2,6,8,13,15	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	10,12,17,18	2,6,8,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	10,12,16	2,6,8	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	10,12,17	2,6,8,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	10,12,16,18	2,6,8,15,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	10,12,14	2,6,8	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	10,12,14,16,17,18	2,6,8,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	10,12,14,18	2,6,8,15,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	10,12,14,16,17	2,6,8,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	10,12,17	2,6,8,13,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	10,12,16,18	2,6,8,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	10,12,17,18	2,6,8,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	10,12,16	2,6,8,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	10,12,14,18	2,6,8,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	10,12,14,16,17	2,6,8,13,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	10,12,14	2,6,8,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	10,12,14,16,17,18	2,6,8,13,15,17,18	2^{-12}

Table 0.556 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	10,18	2,6,8,11,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	10,16,17	2,6,8,11,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	10	2,6,8,11,15	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	10,16,17,18	2,6,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	10,14,17	2,6,8,11,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	10,14,16,18	2,6,8,11,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	10,14,17,18	2,6,8,11,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	10,14,16	2,6,8,11,15	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	10	2,6,8,11,13	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	10,16,17,18	2,6,8,11,13,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	10,18	2,6,8,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	10,16,17	2,6,8,11,13,15,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	10,14,17,18	2,6,8,11,13,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	10,14,16	2,6,8,11,13	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	10,14,17	2,6,8,11,13,15,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	10,14,16,18	2,6,8,11,13,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	10,12,17	2,6,8,11,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	10,12,16,18	2,6,8,11,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	10,12,17,18	2,6,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	10,12,16	2,6,8,11,15	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	10,12,14,18	2,6,8,11,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	10,12,14,16,17	2,6,8,11,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	10,12,14	2,6,8,11,15	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	10,12,14,16,17,18	2,6,8,11,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	10,12,17,18	2,6,8,11,13,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	10,12,16	2,6,8,11,13	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	10,12,17	2,6,8,11,13,15,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	10,12,16,18	2,6,8,11,13,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	10,12,14	2,6,8,11,13	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	10,12,14,16,17,18	2,6,8,11,13,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	10,12,14,18	2,6,8,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	10,12,14,16,17	2,6,8,11,13,15,17	2^{-12}

Table 0.557 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	17	2,6,8,9,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	16,18	2,6,8,9,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	17,18	2,6,8,9,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	16	2,6,8,9,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	14,18	2,6,8,9,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	14,16,17	2,6,8,9,17	2^{-1}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	14	2,6,8,9,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	14,16,17,18	2,6,8,9,15,17,18	2^{-1}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	17,18	2,6,8,9,13,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	16	2,6,8,9,13	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	17	2,6,8,9,13,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	16,18	2,6,8,9,13,15,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	14	2,6,8,9,13	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	14,16,17,18	2,6,8,9,13,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	14,18	2,6,8,9,13,15,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	14,16,17	2,6,8,9,13,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	12,18	2,6,8,9,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	12,16,17	2,6,8,9,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	12	2,6,8,9,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	12,16,17,18	2,6,8,9,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	12,14,17	2,6,8,9,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	12,14,16,18	2,6,8,9,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	12,14,17,18	2,6,8,9,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	12,14,16	2,6,8,9,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	12	2,6,8,9,13	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	12,16,17,18	2,6,8,9,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	12,18	2,6,8,9,13,15,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	12,16,17	2,6,8,9,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	12,14,17,18	2,6,8,9,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	12,14,16	2,6,8,9,13	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	12,14,17	2,6,8,9,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	12,14,16,18	2,6,8,9,13,15,18	2^{-12}

Table 0.558 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	17,18	2,6,8,9,11,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	16	2,6,8,9,11	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	17	2,6,8,9,11,15,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	16,18	2,6,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	14	2,6,8,9,11	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	14,16,17,18	2,6,8,9,11,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	14,18	2,6,8,9,11,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	14,16,17	2,6,8,9,11,15,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	17	2,6,8,9,11,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	16,18	2,6,8,9,11,13,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	17,18	2,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	16	2,6,8,9,11,13,15	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	14,18	2,6,8,9,11,13,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	14,16,17	2,6,8,9,11,13,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	14	2,6,8,9,11,13,15	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	14,16,17,18	2,6,8,9,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	12	2,6,8,9,11	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	12,16,17,18	2,6,8,9,11,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	12,18	2,6,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	12,16,17	2,6,8,9,11,15,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	12,14,17,18	2,6,8,9,11,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	12,14,16	2,6,8,9,11	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	12,14,17	2,6,8,9,11,15,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	12,14,16,18	2,6,8,9,11,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	12,18	2,6,8,9,11,13,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	12,16,17	2,6,8,9,11,13,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	12	2,6,8,9,11,13,15	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	12,16,17,18	2,6,8,9,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	12,14,17	2,6,8,9,11,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	12,14,16,18	2,6,8,9,11,13,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	12,14,17,18	2,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	12,14,16	2,6,8,9,11,13,15	2^{-12}

Table 0.559 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	10,18	2,6,8,9,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	10,16,17	2,6,8,9,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	10	2,6,8,9,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	10,16,17,18	2,6,8,9,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	10,14,17	2,6,8,9,17	2^{-34}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	10,14,16,18	2,6,8,9,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	10,14,17,18	2,6,8,9,15,17,18	2^{-34}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	10,14,16	2,6,8,9,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	10	2,6,8,9,13	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	10,16,17,18	2,6,8,9,13,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	10,18	2,6,8,9,13,15,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	10,16,17	2,6,8,9,13,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	10,14,17,18	2,6,8,9,13,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	10,14,16	2,6,8,9,13	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	10,14,17	2,6,8,9,13,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	10,14,16,18	2,6,8,9,13,15,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	10,12,17	2,6,8,9,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	10,12,16,18	2,6,8,9,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	10,12,17,18	2,6,8,9,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	10,12,16	2,6,8,9,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	10,12,14,18	2,6,8,9,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	10,12,14,16,17	2,6,8,9,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	10,12,14	2,6,8,9,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	10,12,14,16,17,18	2,6,8,9,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	10,12,17,18	2,6,8,9,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	10,12,16	2,6,8,9,13	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	10,12,17	2,6,8,9,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	10,12,16,18	2,6,8,9,13,15,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	10,12,14	2,6,8,9,13	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	10,12,14,16,17,18	2,6,8,9,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	10,12,14,18	2,6,8,9,13,15,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	10,12,14,16,17	2,6,8,9,13,15,17	$2^{-17.5}$

Table 0.560 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	10	2,6,8,9,11	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	10,16,17,18	2,6,8,9,11,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	10,18	2,6,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	10,16,17	2,6,8,9,11,15,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	10,14,17,18	2,6,8,9,11,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	10,14,16	2,6,8,9,11	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	10,14,17	2,6,8,9,11,15,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	10,14,16,18	2,6,8,9,11,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	10,18	2,6,8,9,11,13,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	10,16,17	2,6,8,9,11,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	10	2,6,8,9,11,13,15	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	10,16,17,18	2,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	10,14,17	2,6,8,9,11,13,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	10,14,16,18	2,6,8,9,11,13,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	10,14,17,18	2,6,8,9,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	10,14,16	2,6,8,9,11,13,15	2^{-12}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	10,12,17,18	2,6,8,9,11,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	10,12,16	2,6,8,9,11	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	10,12,17	2,6,8,9,11,15,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	10,12,16,18	2,6,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	10,12,14	2,6,8,9,11	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	10,12,14,16,17,18	2,6,8,9,11,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	10,12,14,18	2,6,8,9,11,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	10,12,14,16,17	2,6,8,9,11,15,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	10,12,17	2,6,8,9,11,13,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	10,12,16,18	2,6,8,9,11,13,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	10,12,17,18	2,6,8,9,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	10,12,16	2,6,8,9,11,13,15	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	10,12,14,18	2,6,8,9,11,13,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	10,12,14,16,17	2,6,8,9,11,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	10,12,14	2,6,8,9,11,13,15	2^{-23}
$(0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	10,12,14,16,17,18	2,6,8,9,11,13,15,17,18	$2^{-17.5}$

Table 0.561 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	7,18	2,6,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	7,16,17	2,6,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	7	2,6,15	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	7,16,17,18	2,6,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	7,14,17	2,6,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	7,14,16,18	2,6,18	2^{-34}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	7,14,17,18	2,6,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	7,14,16	2,6,15	2^{-34}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	7	2,6,13	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	7,16,17,18	2,6,13,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	7,18	2,6,13,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	7,16,17	2,6,13,15,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	7,14,17,18	2,6,13,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	7,14,16	2,6,13	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	7,14,17	2,6,13,15,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	7,14,16,18	2,6,13,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	7,12,17	2,6,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	7,12,16,18	2,6,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	7,12,17,18	2,6,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	7,12,16	2,6,15	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	7,12,14,18	2,6,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	7,12,14,16,17	2,6,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	7,12,14	2,6,15	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	7,12,14,16,17,18	2,6,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	7,12,17,18	2,6,13,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	7,12,16	2,6,13	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	7,12,17	2,6,13,15,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	7,12,16,18	2,6,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	7,12,14	2,6,13	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	7,12,14,16,17,18	2,6,13,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	7,12,14,18	2,6,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	7,12,14,16,17	2,6,13,15,17	2^{-23}

Table 0.562 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	7	2,6,11	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	7,16,17,18	2,6,11,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	7,18	2,6,11,15,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	7,16,17	2,6,11,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	7,14,17,18	2,6,11,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	7,14,16	2,6,11	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	7,14,17	2,6,11,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	7,14,16,18	2,6,11,15,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	7,18	2,6,11,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	7,16,17	2,6,11,13,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	7	2,6,11,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	7,16,17,18	2,6,11,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	7,14,17	2,6,11,13,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	7,14,16,18	2,6,11,13,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	7,14,17,18	2,6,11,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	7,14,16	2,6,11,13,15	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	7,12,17,18	2,6,11,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	7,12,16	2,6,11	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	7,12,17	2,6,11,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	7,12,16,18	2,6,11,15,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	7,12,14	2,6,11	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	7,12,14,16,17,18	2,6,11,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	7,12,14,18	2,6,11,15,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	7,12,14,16,17	2,6,11,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	7,12,17	2,6,11,13,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	7,12,16,18	2,6,11,13,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	7,12,17,18	2,6,11,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	7,12,16	2,6,11,13,15	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	7,12,14,18	2,6,11,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	7,12,14,16,17	2,6,11,13,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	7,12,14	2,6,11,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	7,12,14,16,17,18	2,6,11,13,15,17,18	2^{-23}

Table 0.563 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(2)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	7,10,17	2,6,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	7,10,16,18	2,6,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	7,10,17,18	2,6,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	7,10,16	2,6,15	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	7,10,14,18	2,6,18	2^{-1}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	7,10,14,16,17	2,6,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	7,10,14	2,6,15	2^{-1}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	7,10,14,16,17,18	2,6,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	7,10,17,18	2,6,13,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	7,10,16	2,6,13	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	7,10,17	2,6,13,15,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	7,10,16,18	2,6,13,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	7,10,14	2,6,13	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	7,10,14,16,17,18	2,6,13,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	7,10,14,18	2,6,13,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	7,10,14,16,17	2,6,13,15,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	7,10,12,18	2,6,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	7,10,12,16,17	2,6,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	7,10,12	2,6,15	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	7,10,12,16,17,18	2,6,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	7,10,12,14,17	2,6,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	7,10,12,14,16,18	2,6,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	7,10,12,14,17,18	2,6,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	7,10,12,14,16	2,6,15	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	7,10,12	2,6,13	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	7,10,12,16,17,18	2,6,13,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	7,10,12,18	2,6,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	7,10,12,16,17	2,6,13,15,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	7,10,12,14,17,18	2,6,13,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	7,10,12,14,16	2,6,13	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	7,10,12,14,17	2,6,13,15,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	7,10,12,14,16,18	2,6,13,15,18	$2^{-17.5}$

Table 0.564 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	7,10,17,18	2,6,11,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	7,10,16	2,6,11	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	7,10,17	2,6,11,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	7,10,16,18	2,6,11,15,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	7,10,14	2,6,11	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	7,10,14,16,17,18	2,6,11,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	7,10,14,18	2,6,11,15,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	7,10,14,16,17	2,6,11,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	7,10,17	2,6,11,13,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	7,10,16,18	2,6,11,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	7,10,17,18	2,6,11,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	7,10,16	2,6,11,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	7,10,14,18	2,6,11,13,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	7,10,14,16,17	2,6,11,13,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	7,10,14	2,6,11,13,15	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	7,10,14,16,17,18	2,6,11,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	7,10,12	2,6,11	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	7,10,12,16,17,18	2,6,11,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	7,10,12,18	2,6,11,15,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	7,10,12,16,17	2,6,11,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	7,10,12,14,17,18	2,6,11,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	7,10,12,14,16	2,6,11	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	7,10,12,14,17	2,6,11,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	7,10,12,14,16,18	2,6,11,15,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	7,10,12,18	2,6,11,13,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	7,10,12,16,17	2,6,11,13,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	7,10,12	2,6,11,13,15	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	7,10,12,16,17,18	2,6,11,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	7,10,12,14,17	2,6,11,13,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	7,10,12,14,16,18	2,6,11,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	7,10,12,14,17,18	2,6,11,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	7,10,12,14,16	2,6,11,13,15	$2^{-17.5}$

Table 0.565 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	7	2,6,9	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	7,16,17,18	2,6,9,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	7,18	2,6,9,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	7,16,17	2,6,9,15,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	7,14,17,18	2,6,9,17,18	2^{-1}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	7,14,16	2,6,9	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	7,14,17	2,6,9,15,17	2^{-1}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	7,14,16,18	2,6,9,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	7,18	2,6,9,13,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	7,16,17	2,6,9,13,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	7	2,6,9,13,15	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	7,16,17,18	2,6,9,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	7,14,17	2,6,9,13,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	7,14,16,18	2,6,9,13,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	7,14,17,18	2,6,9,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	7,14,16	2,6,9,13,15	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	7,12,17,18	2,6,9,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	7,12,16	2,6,9	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	7,12,17	2,6,9,15,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	7,12,16,18	2,6,9,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	7,12,14	2,6,9	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	7,12,14,16,17,18	2,6,9,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	7,12,14,18	2,6,9,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	7,12,14,16,17	2,6,9,15,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	7,12,17	2,6,9,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	7,12,16,18	2,6,9,13,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	7,12,17,18	2,6,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	7,12,16	2,6,9,13,15	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	7,12,14,18	2,6,9,13,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	7,12,14,16,17	2,6,9,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	7,12,14	2,6,9,13,15	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	7,12,14,16,17,18	2,6,9,13,15,17,18	$2^{-17.5}$

Table 0.566 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	7,18	2,6,9,11,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	7,16,17	2,6,9,11,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	7	2,6,9,11,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	7,16,17,18	2,6,9,11,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	7,14,17	2,6,9,11,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	7,14,16,18	2,6,9,11,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	7,14,17,18	2,6,9,11,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	7,14,16	2,6,9,11,15	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	7	2,6,9,11,13	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	7,16,17,18	2,6,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	7,18	2,6,9,11,13,15,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	7,16,17	2,6,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	7,14,17,18	2,6,9,11,13,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	7,14,16	2,6,9,11,13	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	7,14,17	2,6,9,11,13,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	7,14,16,18	2,6,9,11,13,15,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	7,12,17	2,6,9,11,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	7,12,16,18	2,6,9,11,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	7,12,17,18	2,6,9,11,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	7,12,16	2,6,9,11,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	7,12,14,18	2,6,9,11,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	7,12,14,16,17	2,6,9,11,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	7,12,14	2,6,9,11,15	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	7,12,14,16,17,18	2,6,9,11,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	7,12,17,18	2,6,9,11,13,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	7,12,16	2,6,9,11,13	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	7,12,17	2,6,9,11,13,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	7,12,16,18	2,6,9,11,13,15,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	7,12,14	2,6,9,11,13	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	7,12,14,16,17,18	2,6,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	7,12,14,18	2,6,9,11,13,15,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	7,12,14,16,17	2,6,9,11,13,15,17	$2^{-17.5}$

Table 0.567 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	7,10,17,18	2,6,9,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	7,10,16	2,6,9	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	7,10,17	2,6,9,15,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	7,10,16,18	2,6,9,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	7,10,14	2,6,9	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	7,10,14,16,17,18	2,6,9,17,18	2^{-34}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	7,10,14,18	2,6,9,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	7,10,14,16,17	2,6,9,15,17	2^{-34}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	7,10,17	2,6,9,13,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	7,10,16,18	2,6,9,13,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	7,10,17,18	2,6,9,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	7,10,16	2,6,9,13,15	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	7,10,14,18	2,6,9,13,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	7,10,14,16,17	2,6,9,13,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	7,10,14	2,6,9,13,15	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	7,10,14,16,17,18	2,6,9,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	7,10,12	2,6,9	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	7,10,12,16,17,18	2,6,9,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	7,10,12,18	2,6,9,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	7,10,12,16,17	2,6,9,15,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	7,10,12,14,17,18	2,6,9,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	7,10,12,14,16	2,6,9	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	7,10,12,14,17	2,6,9,15,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	7,10,12,14,16,18	2,6,9,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	7,10,12,18	2,6,9,13,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	7,10,12,16,17	2,6,9,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	7,10,12	2,6,9,13,15	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	7,10,12,16,17,18	2,6,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	7,10,12,14,17	2,6,9,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	7,10,12,14,16,18	2,6,9,13,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	7,10,12,14,17,18	2,6,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	7,10,12,14,16	2,6,9,13,15	2^{-23}

Table 0.568 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	7,10,17	2,6,9,11,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	7,10,16,18	2,6,9,11,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	7,10,17,18	2,6,9,11,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	7,10,16	2,6,9,11,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	7,10,14,18	2,6,9,11,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	7,10,14,16,17	2,6,9,11,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	7,10,14	2,6,9,11,15	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	7,10,14,16,17,18	2,6,9,11,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	7,10,17,18	2,6,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	7,10,16	2,6,9,11,13	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	7,10,17	2,6,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	7,10,16,18	2,6,9,11,13,15,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	7,10,14	2,6,9,11,13	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	7,10,14,16,17,18	2,6,9,11,13,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	7,10,14,18	2,6,9,11,13,15,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	7,10,14,16,17	2,6,9,11,13,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	7,10,12,18	2,6,9,11,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	7,10,12,16,17	2,6,9,11,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	7,10,12	2,6,9,11,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	7,10,12,16,17,18	2,6,9,11,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	7,10,12,14,17	2,6,9,11,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	7,10,12,14,16,18	2,6,9,11,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	7,10,12,14,17,18	2,6,9,11,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	7,10,12,14,16	2,6,9,11,15	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	7,10,12	2,6,9,11,13	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	7,10,12,16,17,18	2,6,9,11,13,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	7,10,12,18	2,6,9,11,13,15,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	7,10,12,16,17	2,6,9,11,13,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	7,10,12,14,17,18	2,6,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	7,10,12,14,16	2,6,9,11,13	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	7,10,12,14,17	2,6,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	7,10,12,14,16,18	2,6,9,11,13,15,18	2^{-23}

Table 0.569 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	7,17	2,6,8,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	7,16,18	2,6,8,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	7,17,18	2,6,8,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	7,16	2,6,8,15	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	7,14,18	2,6,8,18	2^{-34}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	7,14,16,17	2,6,8,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	7,14	2,6,8,15	2^{-34}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	7,14,16,17,18	2,6,8,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	7,17,18	2,6,8,13,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	7,16	2,6,8,13	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	7,17	2,6,8,13,15,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	7,16,18	2,6,8,13,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	7,14	2,6,8,13	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	7,14,16,17,18	2,6,8,13,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	7,14,18	2,6,8,13,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	7,14,16,17	2,6,8,13,15,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	7,12,18	2,6,8,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	7,12,16,17	2,6,8,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	7,12	2,6,8,15	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	7,12,16,17,18	2,6,8,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	7,12,14,17	2,6,8,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	7,12,14,16,18	2,6,8,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	7,12,14,17,18	2,6,8,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	7,12,14,16	2,6,8,15	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	7,12	2,6,8,13	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	7,12,16,17,18	2,6,8,13,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	7,12,18	2,6,8,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	7,12,16,17	2,6,8,13,15,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	7,12,14,17,18	2,6,8,13,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	7,12,14,16	2,6,8,13	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	7,12,14,17	2,6,8,13,15,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	7,12,14,16,18	2,6,8,13,15,18	$2^{-17.5}$

Table 0.570 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	7,17,18	2,6,8,11,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	7,16	2,6,8,11	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	7,17	2,6,8,11,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	7,16,18	2,6,8,11,15,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	7,14	2,6,8,11	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	7,14,16,17,18	2,6,8,11,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	7,14,18	2,6,8,11,15,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	7,14,16,17	2,6,8,11,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	7,17	2,6,8,11,13,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	7,16,18	2,6,8,11,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	7,17,18	2,6,8,11,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	7,16	2,6,8,11,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	7,14,18	2,6,8,11,13,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	7,14,16,17	2,6,8,11,13,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	7,14	2,6,8,11,13,15	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	7,14,16,17,18	2,6,8,11,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	7,12	2,6,8,11	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	7,12,16,17,18	2,6,8,11,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	7,12,18	2,6,8,11,15,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	7,12,16,17	2,6,8,11,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	7,12,14,17,18	2,6,8,11,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	7,12,14,16	2,6,8,11	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	7,12,14,17	2,6,8,11,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	7,12,14,16,18	2,6,8,11,15,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	7,12,18	2,6,8,11,13,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	7,12,16,17	2,6,8,11,13,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	7,12	2,6,8,11,13,15	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	7,12,16,17,18	2,6,8,11,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	7,12,14,17	2,6,8,11,13,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	7,12,14,16,18	2,6,8,11,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	7,12,14,17,18	2,6,8,11,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	7,12,14,16	2,6,8,11,13,15	$2^{-17.5}$

Table 0.571 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	7,10,18	2,6,8,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	7,10,16,17	2,6,8,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	7,10	2,6,8,15	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	7,10,16,17,18	2,6,8,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	7,10,14,17	2,6,8,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	7,10,14,16,18	2,6,8,18	2^{-1}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	7,10,14,17,18	2,6,8,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	7,10,14,16	2,6,8,15	2^{-1}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	7,10	2,6,8,13	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	7,10,16,17,18	2,6,8,13,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	7,10,18	2,6,8,13,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	7,10,16,17	2,6,8,13,15,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	7,10,14,17,18	2,6,8,13,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	7,10,14,16	2,6,8,13	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	7,10,14,17	2,6,8,13,15,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	7,10,14,16,18	2,6,8,13,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	7,10,12,17	2,6,8,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	7,10,12,16,18	2,6,8,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	7,10,12,17,18	2,6,8,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	7,10,12,16	2,6,8,15	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	7,10,12,14,18	2,6,8,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	7,10,12,14,16,17	2,6,8,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	7,10,12,14	2,6,8,15	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	7,10,12,14,16,17,18	2,6,8,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	7,10,12,17,18	2,6,8,13,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	7,10,12,16	2,6,8,13	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	7,10,12,17	2,6,8,13,15,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	7,10,12,16,18	2,6,8,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	7,10,12,14	2,6,8,13	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	7,10,12,14,16,17,18	2,6,8,13,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	7,10,12,14,18	2,6,8,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	7,10,12,14,16,17	2,6,8,13,15,17	2^{-12}

Table 0.572 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	7,10	2,6,8,11	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	7,10,16,17,18	2,6,8,11,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	7,10,18	2,6,8,11,15,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	7,10,16,17	2,6,8,11,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	7,10,14,17,18	2,6,8,11,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	7,10,14,16	2,6,8,11	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	7,10,14,17	2,6,8,11,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	7,10,14,16,18	2,6,8,11,15,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	7,10,18	2,6,8,11,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	7,10,16,17	2,6,8,11,13,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	7,10	2,6,8,11,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	7,10,16,17,18	2,6,8,11,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	7,10,14,17	2,6,8,11,13,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	7,10,14,16,18	2,6,8,11,13,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	7,10,14,17,18	2,6,8,11,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	7,10,14,16	2,6,8,11,13,15	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	7,10,12,17,18	2,6,8,11,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	7,10,12,16	2,6,8,11	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	7,10,12,17	2,6,8,11,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	7,10,12,16,18	2,6,8,11,15,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	7,10,12,14	2,6,8,11	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	7,10,12,14,16,17,18	2,6,8,11,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	7,10,12,14,18	2,6,8,11,15,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	7,10,12,14,16,17	2,6,8,11,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	7,10,12,17	2,6,8,11,13,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	7,10,12,16,18	2,6,8,11,13,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	7,10,12,17,18	2,6,8,11,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	7,10,12,16	2,6,8,11,13,15	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	7,10,12,14,18	2,6,8,11,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	7,10,12,14,16,17	2,6,8,11,13,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	7,10,12,14	2,6,8,11,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	7,10,12,14,16,17,18	2,6,8,11,13,15,17,18	2^{-12}

Table 0.573 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	7,17,18	2,6,8,9,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	7,16	2,6,8,9	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	7,17	2,6,8,9,15,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	7,16,18	2,6,8,9,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	7,14	2,6,8,9	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	7,14,16,17,18	2,6,8,9,17,18	2^{-1}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	7,14,18	2,6,8,9,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	7,14,16,17	2,6,8,9,15,17	2^{-1}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	7,17	2,6,8,9,13,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	7,16,18	2,6,8,9,13,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	7,17,18	2,6,8,9,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	7,16	2,6,8,9,13,15	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	7,14,18	2,6,8,9,13,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	7,14,16,17	2,6,8,9,13,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	7,14	2,6,8,9,13,15	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	7,14,16,17,18	2,6,8,9,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	7,12	2,6,8,9	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	7,12,16,17,18	2,6,8,9,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	7,12,18	2,6,8,9,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	7,12,16,17	2,6,8,9,15,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	7,12,14,17,18	2,6,8,9,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	7,12,14,16	2,6,8,9	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	7,12,14,17	2,6,8,9,15,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	7,12,14,16,18	2,6,8,9,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	7,12,18	2,6,8,9,13,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	7,12,16,17	2,6,8,9,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	7,12	2,6,8,9,13,15	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	7,12,16,17,18	2,6,8,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	7,12,14,17	2,6,8,9,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	7,12,14,16,18	2,6,8,9,13,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	7,12,14,17,18	2,6,8,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	7,12,14,16	2,6,8,9,13,15	2^{-12}

Table 0.574 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	7,17	2,6,8,9,11,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	7,16,18	2,6,8,9,11,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	7,17,18	2,6,8,9,11,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	7,16	2,6,8,9,11,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	7,14,18	2,6,8,9,11,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	7,14,16,17	2,6,8,9,11,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	7,14	2,6,8,9,11,15	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	7,14,16,17,18	2,6,8,9,11,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	7,17,18	2,6,8,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	7,16	2,6,8,9,11,13	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	7,17	2,6,8,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	7,16,18	2,6,8,9,11,13,15,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	7,14	2,6,8,9,11,13	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	7,14,16,17,18	2,6,8,9,11,13,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	7,14,18	2,6,8,9,11,13,15,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	7,14,16,17	2,6,8,9,11,13,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	7,12,18	2,6,8,9,11,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	7,12,16,17	2,6,8,9,11,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	7,12	2,6,8,9,11,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	7,12,16,17,18	2,6,8,9,11,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	7,12,14,17	2,6,8,9,11,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	7,12,14,16,18	2,6,8,9,11,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	7,12,14,17,18	2,6,8,9,11,15,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	7,12,14,16	2,6,8,9,11,15	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	7,12	2,6,8,9,11,13	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	7,12,16,17,18	2,6,8,9,11,13,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	7,12,18	2,6,8,9,11,13,15,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	7,12,16,17	2,6,8,9,11,13,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	7,12,14,17,18	2,6,8,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	7,12,14,16	2,6,8,9,11,13	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	7,12,14,17	2,6,8,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	7,12,14,16,18	2,6,8,9,11,13,15,18	2^{-12}

Table 0.575 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	7,10	2,6,8,9	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	7,10,16,17,18	2,6,8,9,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	7,10,18	2,6,8,9,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	7,10,16,17	2,6,8,9,15,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	7,10,14,17,18	2,6,8,9,17,18	2^{-34}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	7,10,14,16	2,6,8,9	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	7,10,14,17	2,6,8,9,15,17	2^{-34}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	7,10,14,16,18	2,6,8,9,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	7,10,18	2,6,8,9,13,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	7,10,16,17	2,6,8,9,13,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	7,10	2,6,8,9,13,15	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	7,10,16,17,18	2,6,8,9,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	7,10,14,17	2,6,8,9,13,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	7,10,14,16,18	2,6,8,9,13,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	7,10,14,17,18	2,6,8,9,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	7,10,14,16	2,6,8,9,13,15	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	7,10,12,17,18	2,6,8,9,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	7,10,12,16	2,6,8,9	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	7,10,12,17	2,6,8,9,15,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	7,10,12,16,18	2,6,8,9,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	7,10,12,14	2,6,8,9	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	7,10,12,14,16,17,18	2,6,8,9,17,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	7,10,12,14,18	2,6,8,9,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	7,10,12,14,16,17	2,6,8,9,15,17	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	7,10,12,17	2,6,8,9,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	7,10,12,16,18	2,6,8,9,13,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	7,10,12,14,18	2,6,8,9,13,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	7,10,12,14,16,17	2,6,8,9,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	7,10,12,14,16,17	2,6,8,9,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	7,10,12,14	2,6,8,9,13,15	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	7,10,12,14,16,17,18	2,6,8,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	7,10,12,14,16,17,18	2,6,8,9,13,15,17,18	$2^{-17.5}$

Table 0.576 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	7,10,18	2,6,8,9,11,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	7,10,16,17	2,6,8,9,11,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	7,10	2,6,8,9,11,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	7,10,16,17,18	2,6,8,9,11,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	7,10,14,17	2,6,8,9,11,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	7,10,14,16,18	2,6,8,9,11,18	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	7,10,14,17,18	2,6,8,9,11,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	7,10,14,16	2,6,8,9,11,15	$2^{-6.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	7,10	2,6,8,9,11,13	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	7,10,16,17,18	2,6,8,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	7,10,18	2,6,8,9,11,13,15,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	7,10,16,17	2,6,8,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	7,10,14,17,18	2,6,8,9,11,13,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	7,10,14,16	2,6,8,9,11,13	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	7,10,14,17	2,6,8,9,11,13,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	7,10,14,16,18	2,6,8,9,11,13,15,18	2^{-12}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	7,10,12,17	2,6,8,9,11,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	7,10,12,16,18	2,6,8,9,11,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	7,10,12,17,18	2,6,8,9,11,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	7,10,12,16	2,6,8,9,11,15	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	7,10,12,14,18	2,6,8,9,11,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	7,10,12,14,16,17	2,6,8,9,11,17	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	7,10,12,14	2,6,8,9,11,15	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	7,10,12,14,16,17,18	2,6,8,9,11,15,17,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	7,10,12,17,18	2,6,8,9,11,13,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	7,10,12,16	2,6,8,9,11,13	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	7,10,12,17	2,6,8,9,11,13,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	7,10,12,16,18	2,6,8,9,11,13,15,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	7,10,12,14	2,6,8,9,11,13	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	7,10,12,14,16,17,18	2,6,8,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	7,10,12,14,18	2,6,8,9,11,13,15,18	2^{-23}
$(0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	7,10,12,14,16,17	2,6,8,9,11,13,15,17	$2^{-17.5}$

Table 0.577 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	5,17	2,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	5,16,18	2,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	5,17,18	2,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	5,16	2,15	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	5,14,18	2,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	5,14,16,17	2,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	5,14	2,15	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	5,14,16,17,18	2,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	5,17,18	2,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	5,16	2,13	2^{-34}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	5,17	2,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	5,16,18	2,13,15,18	2^{-34}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	5,14	2,13	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	5,14,16,17,18	2,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	5,14,18	2,13,15,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	5,14,16,17	2,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	5,12,18	2,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	5,12,16,17	2,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	5,12	2,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	5,12,16,17,18	2,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	5,12,14,17	2,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	5,12,14,16,18	2,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	5,12,14,17,18	2,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	5,12,14,16	2,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	5,12	2,13	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	5,12,16,17,18	2,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	5,12,18	2,13,15,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	5,12,16,17	2,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	5,12,14,17,18	2,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	5,12,14,16	2,13	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	5,12,14,17	2,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	5,12,14,16,18	2,13,15,18	2^{-23}

Table 0.578 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	5,17,18	2,11,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	5,16	2,11	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	5,17	2,11,15,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	5,16,18	2,11,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	5,14	2,11	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	5,14,16,17,18	2,11,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	5,14,18	2,11,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	5,14,16,17	2,11,15,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	5,17	2,11,13,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	5,16,18	2,11,13,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	5,17,18	2,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	5,16	2,11,13,15	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	5,14,18	2,11,13,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	5,14,16,17	2,11,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	5,14	2,11,13,15	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	5,14,16,17,18	2,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	5,12	2,11	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	5,12,16,17,18	2,11,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	5,12,18	2,11,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	5,12,16,17	2,11,15,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	5,12,14,17,18	2,11,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	5,12,14,16	2,11	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	5,12,14,17	2,11,15,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	5,12,14,16,18	2,11,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	5,12,18	2,11,13,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	5,12,16,17	2,11,13,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	5,12	2,11,13,15	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	5,12,16,17,18	2,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	5,12,14,17	2,11,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	5,12,14,16,18	2,11,13,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	5,12,14,17,18	2,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	5,12,14,16	2,11,13,15	2^{-23}

Table 0.579 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	5,10,18	2,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	5,10,16,17	2,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	5,10	2,15	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	5,10,16,17,18	2,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	5,10,14,17	2,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	5,10,14,16,18	2,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	5,10,14,17,18	2,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	5,10,14,16	2,15	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	5,10	2,13	2^{-1}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	5,10,16,17,18	2,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	5,10,18	2,13,15,18	2^{-1}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	5,10,16,17	2,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	5,10,14,17,18	2,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	5,10,14,16	2,13	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	5,10,14,17	2,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	5,10,14,16,18	2,13,15,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	5,10,12,17	2,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	5,10,12,16,18	2,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	5,10,12,17,18	2,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	5,10,12,16	2,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	5,10,12,14,18	2,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	5,10,12,14,16,17	2,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	5,10,12,14	2,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	5,10,12,14,16,17,18	2,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	5,10,12,17,18	2,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	5,10,12,16	2,13	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	5,10,12,17	2,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	5,10,12,16,18	2,13,15,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	5,10,12,14	2,13	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	5,10,12,14,16,17,18	2,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	5,10,12,14,18	2,13,15,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	5,10,12,14,16,17	2,13,15,17	$2^{-17.5}$

Table 0.580 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	5,10	2,11	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	5,10,16,17,18	2,11,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	5,10,18	2,11,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	5,10,16,17	2,11,15,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	5,10,14,17,18	2,11,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	5,10,14,16	2,11	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	5,10,14,17	2,11,15,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	5,10,14,16,18	2,11,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	5,10,18	2,11,13,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	5,10,16,17	2,11,13,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	5,10	2,11,13,15	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	5,10,16,17,18	2,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	5,10,14,17	2,11,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	5,10,14,16,18	2,11,13,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	5,10,14,17,18	2,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	5,10,14,16	2,11,13,15	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	5,10,12,17,18	2,11,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	5,10,12,16	2,11	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	5,10,12,17	2,11,15,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	5,10,12,16,18	2,11,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	5,10,12,14	2,11	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	5,10,12,14,16,17,18	2,11,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	5,10,12,14,18	2,11,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	5,10,12,14,16,17	2,11,15,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	5,10,12,17	2,11,13,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	5,10,12,16,18	2,11,13,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	5,10,12,17,18	2,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	5,10,12,16	2,11,13,15	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	5,10,12,14,18	2,11,13,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	5,10,12,14,16,17	2,11,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	5,10,12,14	2,11,13,15	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	5,10,12,14,16,17,18	2,11,13,15,17,18	$2^{-17.5}$

Table 0.581 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	5,17,18	2,9,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	5,16	2,9	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	5,17	2,9,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	5,16,18	2,9,15,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	5,14	2,9	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	5,14,16,17,18	2,9,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	5,14,18	2,9,15,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	5,14,16,17	2,9,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	5,17	2,9,13,17	2^{-1}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	5,16,18	2,9,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	5,17,18	2,9,13,15,17,18	2^{-1}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	5,16	2,9,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	5,14,18	2,9,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	5,14,16,17	2,9,13,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	5,14	2,9,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	5,14,16,17,18	2,9,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	5,12	2,9	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	5,12,16,17,18	2,9,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	5,12,18	2,9,15,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	5,12,16,17	2,9,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	5,12,14,17,18	2,9,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	5,12,14,16	2,9	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	5,12,14,17	2,9,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	5,12,14,16,18	2,9,15,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	5,12,18	2,9,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	5,12,16,17	2,9,13,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	5,12	2,9,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	5,12,16,17,18	2,9,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	5,12,14,17	2,9,13,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	5,12,14,16,18	2,9,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	5,12,14,17,18	2,9,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	5,12,14,16	2,9,13,15	$2^{-17.5}$

Table 0.582 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	5,17	2,9,11,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	5,16,18	2,9,11,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	5,17,18	2,9,11,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	5,16	2,9,11,15	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	5,14,18	2,9,11,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	5,14,16,17	2,9,11,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	5,14	2,9,11,15	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	5,14,16,17,18	2,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	5,17,18	2,9,11,13,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	5,16	2,9,11,13	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	5,17	2,9,11,13,15,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	5,16,18	2,9,11,13,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	5,14	2,9,11,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	5,14,16,17,18	2,9,11,13,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	5,14,18	2,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	5,14,16,17	2,9,11,13,15,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	5,12,18	2,9,11,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	5,12,16,17	2,9,11,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	5,12	2,9,11,15	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	5,12,16,17,18	2,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	5,12,14,17	2,9,11,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	5,12,14,16,18	2,9,11,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	5,12,14,17,18	2,9,11,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	5,12,14,16	2,9,11,15	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	5,12	2,9,11,13	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	5,12,16,17,18	2,9,11,13,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	5,12,18	2,9,11,13,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	5,12,16,17	2,9,11,13,15,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	5,12,14,17,18	2,9,11,13,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	5,12,14,16	2,9,11,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	5,12,14,17	2,9,11,13,15,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	5,12,14,16,18	2,9,11,13,15,18	$2^{-17.5}$

Table 0.583 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	5,10	2,9	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	5,10,16,17,18	2,9,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	5,10,18	2,9,15,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	5,10,16,17	2,9,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	5,10,14,17,18	2,9,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	5,10,14,16	2,9	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	5,10,14,17	2,9,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	5,10,14,16,18	2,9,15,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	5,10,18	2,9,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	5,10,16,17	2,9,13,17	2^{-34}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	5,10	2,9,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	5,10,16,17,18	2,9,13,15,17,18	2^{-34}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	5,10,14,17	2,9,13,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	5,10,14,16,18	2,9,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	5,10,14,17,18	2,9,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	5,10,14,16	2,9,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	5,10,12,17,18	2,9,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	5,10,12,16	2,9	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	5,10,12,17	2,9,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	5,10,12,16,18	2,9,15,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	5,10,12,14	2,9	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	5,10,12,14,16,17,18	2,9,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	5,10,12,14,18	2,9,15,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	5,10,12,14,16,17	2,9,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	5,10,12,17	2,9,13,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	5,10,12,16,18	2,9,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	5,10,12,17,18	2,9,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	5,10,12,16	2,9,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	5,10,12,14,18	2,9,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	5,10,12,14,16,17	2,9,13,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	5,10,12,14	2,9,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	5,10,12,14,16,17,18	2,9,13,15,17,18	2^{-23}

Table 0.584 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	5,10,18	2,9,11,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	5,10,16,17	2,9,11,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	5,10	2,9,11,15	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	5,10,16,17,18	2,9,11,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	5,10,14,17	2,9,11,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	5,10,14,16,18	2,9,11,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	5,10,14,17,18	2,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	5,10,14,16	2,9,11,15	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	5,10	2,9,11,13	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	5,10,16,17,18	2,9,11,13,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	5,10,18	2,9,11,13,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	5,10,16,17	2,9,11,13,15,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	5,10,14,17,18	2,9,11,13,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	5,10,14,16	2,9,11,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	5,10,14,17	2,9,11,13,15,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	5,10,14,16,18	2,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	5,10,12,17	2,9,11,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	5,10,12,16,18	2,9,11,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	5,10,12,17,18	2,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	5,10,12,16	2,9,11,15	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	5,10,12,14,18	2,9,11,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	5,10,12,14,16,17	2,9,11,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	5,10,12,14	2,9,11,15	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	5,10,12,14,16,17,18	2,9,11,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	5,10,12,17,18	2,9,11,13,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	5,10,12,16	2,9,11,13	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	5,10,12,17	2,9,11,13,15,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	5,10,12,16,18	2,9,11,13,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	5,10,12,14	2,9,11,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	5,10,12,14,16,17,18	2,9,11,13,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	5,10,12,14,18	2,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	5,10,12,14,16,17	2,9,11,13,15,17	2^{-23}

Table 0.585 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	5,18	2,8,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	5,16,17	2,8,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	5	2,8,15	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	5,16,17,18	2,8,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	5,14,17	2,8,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	5,14,16,18	2,8,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	5,14,17,18	2,8,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	5,14,16	2,8,15	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	5	2,8,13	2^{-34}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	5,16,17,18	2,8,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	5,18	2,8,13,15,18	2^{-34}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	5,16,17	2,8,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	5,14,17,18	2,8,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	5,14,16	2,8,13	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	5,14,17	2,8,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	5,14,16,18	2,8,13,15,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	5,12,17	2,8,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	5,12,16,18	2,8,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	5,12,17,18	2,8,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	5,12,16	2,8,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	5,12,14,18	2,8,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	5,12,14,16,17	2,8,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	5,12,14	2,8,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	5,12,14,16,17,18	2,8,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	5,12,17,18	2,8,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	5,12,16	2,8,13	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	5,12,17	2,8,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	5,12,16,18	2,8,13,15,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	5,12,14	2,8,13	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	5,12,14,16,17,18	2,8,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	5,12,14,18	2,8,13,15,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	5,12,14,16,17	2,8,13,15,17	$2^{-17.5}$

Table 0.586 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	5	2,8,11	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	5,16,17,18	2,8,11,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	5,18	2,8,11,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	5,16,17	2,8,11,15,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	5,14,17,18	2,8,11,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	5,14,16	2,8,11	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	5,14,17	2,8,11,15,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	5,14,16,18	2,8,11,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	5,18	2,8,11,13,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	5,16,17	2,8,11,13,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	5	2,8,11,13,15	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	5,16,17,18	2,8,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	5,14,17	2,8,11,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	5,14,16,18	2,8,11,13,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	5,14,17,18	2,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	5,14,16	2,8,11,13,15	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	5,12,17,18	2,8,11,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	5,12,16	2,8,11	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	5,12,17	2,8,11,15,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	5,12,16,18	2,8,11,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	5,12,14	2,8,11	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	5,12,14,16,17,18	2,8,11,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	5,12,14,18	2,8,11,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	5,12,14,16,17	2,8,11,15,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	5,12,17	2,8,11,13,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	5,12,16,18	2,8,11,13,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	5,12,17,18	2,8,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	5,12,16	2,8,11,13,15	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	5,12,14,18	2,8,11,13,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	5,12,14,16,17	2,8,11,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	5,12,14	2,8,11,13,15	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	5,12,14,16,17,18	2,8,11,13,15,17,18	$2^{-17.5}$

Table 0.587 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	5,10,17	2,8,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	5,10,16,18	2,8,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	5,10,17,18	2,8,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	5,10,16	2,8,15	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	5,10,14,18	2,8,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	5,10,14,16,17	2,8,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	5,10,14	2,8,15	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	5,10,14,16,17,18	2,8,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	5,10,17,18	2,8,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	5,10,16	2,8,13	2^{-1}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	5,10,17	2,8,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	5,10,16,18	2,8,13,15,18	2^{-1}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	5,10,14	2,8,13	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	5,10,14,16,17,18	2,8,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	5,10,14,18	2,8,13,15,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	5,10,14,16,17	2,8,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	5,10,12,18	2,8,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	5,10,12,16,17	2,8,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	5,10,12	2,8,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	5,10,12,16,17,18	2,8,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	5,10,12,14,17	2,8,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	5,10,12,14,16,18	2,8,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	5,10,12,14,17,18	2,8,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	5,10,12,14,16	2,8,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	5,10,12	2,8,13	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	5,10,12,16,17,18	2,8,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	5,10,12,18	2,8,13,15,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	5,10,12,16,17	2,8,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	5,10,12,14,17,18	2,8,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	5,10,12,14,16	2,8,13	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	5,10,12,14,17	2,8,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	5,10,12,14,16,18	2,8,13,15,18	2^{-12}

Table 0.588 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	5,10,17,18	2,8,11,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	5,10,16	2,8,11	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	5,10,17	2,8,11,15,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	5,10,16,18	2,8,11,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	5,10,14	2,8,11	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	5,10,14,16,17,18	2,8,11,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	5,10,14,18	2,8,11,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	5,10,14,16,17	2,8,11,15,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	5,10,17	2,8,11,13,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	5,10,16,18	2,8,11,13,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	5,10,17,18	2,8,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	5,10,16	2,8,11,13,15	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	5,10,14,18	2,8,11,13,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	5,10,14,16,17	2,8,11,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	5,10,14	2,8,11,13,15	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	5,10,14,16,17,18	2,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	5,10,12	2,8,11	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	5,10,12,16,17,18	2,8,11,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	5,10,12,18	2,8,11,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	5,10,12,16,17	2,8,11,15,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	5,10,12,14,17,18	2,8,11,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	5,10,12,14,16	2,8,11	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	5,10,12,14,17	2,8,11,15,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	5,10,12,14,16,18	2,8,11,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	5,10,12,18	2,8,11,13,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	5,10,12,16,17	2,8,11,13,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	5,10,12	2,8,11,13,15	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	5,10,12,16,17,18	2,8,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	5,10,12,14,17	2,8,11,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	5,10,12,14,16,18	2,8,11,13,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	5,10,12,14,17,18	2,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	5,10,12,14,16	2,8,11,13,15	2^{-12}

Table 0.589 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	5	2,8,9	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	5,16,17,18	2,8,9,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	5,18	2,8,9,15,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	5,16,17	2,8,9,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	5,14,17,18	2,8,9,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	5,14,16	2,8,9	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	5,14,17	2,8,9,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	5,14,16,18	2,8,9,15,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	5,18	2,8,9,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	5,16,17	2,8,9,13,17	2^{-1}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	5	2,8,9,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	5,16,17,18	2,8,9,13,15,17,18	2^{-1}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	5,14,17	2,8,9,13,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	5,14,16,18	2,8,9,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	5,14,17,18	2,8,9,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	5,14,16	2,8,9,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	5,12,17,18	2,8,9,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	5,12,16	2,8,9	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	5,12,17	2,8,9,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	5,12,16,18	2,8,9,15,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	5,12,14	2,8,9	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	5,12,14,16,17,18	2,8,9,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	5,12,14,18	2,8,9,15,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	5,12,14,16,17	2,8,9,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	5,12,17	2,8,9,13,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	5,12,16,18	2,8,9,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	5,12,17,18	2,8,9,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	5,12,16	2,8,9,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	5,12,14,18	2,8,9,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	5,12,14,16,17	2,8,9,13,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	5,12,14	2,8,9,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	5,12,14,16,17,18	2,8,9,13,15,17,18	2^{-12}

Table 0.590 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	5,18	2,8,9,11,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	5,16,17	2,8,9,11,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	5	2,8,9,11,15	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	5,16,17,18	2,8,9,11,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	5,14,17	2,8,9,11,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	5,14,16,18	2,8,9,11,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	5,14,17,18	2,8,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	5,14,16	2,8,9,11,15	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	5	2,8,9,11,13	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	5,16,17,18	2,8,9,11,13,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	5,18	2,8,9,11,13,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	5,16,17	2,8,9,11,13,15,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	5,14,17,18	2,8,9,11,13,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	5,14,16	2,8,9,11,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	5,14,17	2,8,9,11,13,15,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	5,14,16,18	2,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	5,12,17	2,8,9,11,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	5,12,16,18	2,8,9,11,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	5,12,17,18	2,8,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	5,12,16	2,8,9,11,15	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	5,12,14,18	2,8,9,11,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	5,12,14,16,17	2,8,9,11,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	5,12,14	2,8,9,11,15	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	5,12,14,16,17,18	2,8,9,11,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	5,12,17,18	2,8,9,11,13,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	5,12,16	2,8,9,11,13	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	5,12,17	2,8,9,11,13,15,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	5,12,16,18	2,8,9,11,13,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	5,12,14	2,8,9,11,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	5,12,14,16,17,18	2,8,9,11,13,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	5,12,14,18	2,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	5,12,14,16,17	2,8,9,11,13,15,17	2^{-12}

Table 0.591 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	5,10,17,18	2,8,9,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	5,10,16	2,8,9	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	5,10,17	2,8,9,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	5,10,16,18	2,8,9,15,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	5,10,14	2,8,9	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	5,10,14,16,17,18	2,8,9,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	5,10,14,18	2,8,9,15,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	5,10,14,16,17	2,8,9,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	5,10,17	2,8,9,13,17	2^{-34}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	5,10,16,18	2,8,9,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	5,10,17,18	2,8,9,13,15,17,18	2^{-34}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	5,10,16	2,8,9,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	5,10,14,18	2,8,9,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	5,10,14,16,17	2,8,9,13,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	5,10,14	2,8,9,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	5,10,14,16,17,18	2,8,9,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	5,10,12	2,8,9	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	5,10,12,16,17,18	2,8,9,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	5,10,12,18	2,8,9,15,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	5,10,12,16,17	2,8,9,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	5,10,12,14,17,18	2,8,9,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	5,10,12,14,16	2,8,9	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	5,10,12,14,17	2,8,9,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	5,10,12,14,16,18	2,8,9,15,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	5,10,12,18	2,8,9,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	5,10,12,16,17	2,8,9,13,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	5,10,12	2,8,9,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	5,10,12,16,17,18	2,8,9,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	5,10,12,14,17	2,8,9,13,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	5,10,12,14,16,18	2,8,9,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	5,10,12,14,17,18	2,8,9,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	5,10,12,14,16	2,8,9,13,15	$2^{-17.5}$

Table 0.592 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	5,10,17	2,8,9,11,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	5,10,16,18	2,8,9,11,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	5,10,17,18	2,8,9,11,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	5,10,16	2,8,9,11,15	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	5,10,14,18	2,8,9,11,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	5,10,14,16,17	2,8,9,11,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	5,10,14	2,8,9,11,15	2^{-12}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	5,10,14,16,17,18	2,8,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	5,10,17,18	2,8,9,11,13,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	5,10,16	2,8,9,11,13	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	5,10,17	2,8,9,11,13,15,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	5,10,16,18	2,8,9,11,13,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	5,10,14	2,8,9,11,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	5,10,14,16,17,18	2,8,9,11,13,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	5,10,14,18	2,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	5,10,14,16,17	2,8,9,11,13,15,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	5,10,12,18	2,8,9,11,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	5,10,12,16,17	2,8,9,11,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	5,10,12	2,8,9,11,15	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	5,10,12,16,17,18	2,8,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	5,10,12,14,17	2,8,9,11,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	5,10,12,14,16,18	2,8,9,11,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	5,10,12,14,17,18	2,8,9,11,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	5,10,12,14,16	2,8,9,11,15	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	5,10,12	2,8,9,11,13	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	5,10,12,16,17,18	2,8,9,11,13,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	5,10,12,18	2,8,9,11,13,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	5,10,12,16,17	2,8,9,11,13,15,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	5,10,12,14,17,18	2,8,9,11,13,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	5,10,12,14,16	2,8,9,11,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	5,10,12,14,17	2,8,9,11,13,15,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	5,10,12,14,16,18	2,8,9,11,13,15,18	$2^{-17.5}$

Table 0.593 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	5,7,17,18	2,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	5,7,16	2	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	5,7,17	2,15,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	5,7,16,18	2,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	5,7,14	2	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	5,7,14,16,17,18	2,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	5,7,14,18	2,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	5,7,14,16,17	2,15,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	5,7,17	2,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	5,7,16,18	2,13,18	2^{-34}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	5,7,17,18	2,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	5,7,16	2,13,15	2^{-34}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	5,7,14,18	2,13,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	5,7,14,16,17	2,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	5,7,14	2,13,15	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	5,7,14,16,17,18	2,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	5,7,12	2	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	5,7,12,16,17,18	2,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	5,7,12,18	2,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	5,7,12,16,17	2,15,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	5,7,12,14,17,18	2,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	5,7,12,14,16	2	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	5,7,12,14,17	2,15,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	5,7,12,14,16,18	2,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	5,7,12,18	2,13,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	5,7,12,16,17	2,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	5,7,12	2,13,15	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	5,7,12,16,17,18	2,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	5,7,12,14,17	2,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	5,7,12,14,16,18	2,13,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	5,7,12,14,17,18	2,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	5,7,12,14,16	2,13,15	2^{-23}

Table 0.594 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	5,7,17	2,11,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	5,7,16,18	2,11,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	5,7,17,18	2,11,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	5,7,16	2,11,15	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	5,7,14,18	2,11,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	5,7,14,16,17	2,11,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	5,7,14	2,11,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	5,7,14,16,17,18	2,11,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	5,7,17,18	2,11,13,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	5,7,16	2,11,13	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	5,7,17	2,11,13,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	5,7,16,18	2,11,13,15,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	5,7,14	2,11,13	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	5,7,14,16,17,18	2,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	5,7,14,18	2,11,13,15,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	5,7,14,16,17	2,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	5,7,12,18	2,11,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	5,7,12,16,17	2,11,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	5,7,12	2,11,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	5,7,12,16,17,18	2,11,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	5,7,12,14,17	2,11,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	5,7,12,14,16,18	2,11,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	5,7,12,14,17,18	2,11,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	5,7,12,14,16	2,11,15	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	5,7,12	2,11,13	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	5,7,12,16,17,18	2,11,13,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	5,7,12,18	2,11,13,15,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	5,7,12,16,17	2,11,13,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	5,7,12,14,17,18	2,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	5,7,12,14,16	2,11,13	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	5,7,12,14,17	2,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	5,7,12,14,16,18	2,11,13,15,18	2^{-23}

Table 0.595 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	5,7,10	2	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	5,7,10,16,17,18	2,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	5,7,10,18	2,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	5,7,10,16,17	2,15,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	5,7,10,14,17,18	2,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	5,7,10,14,16	2	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	5,7,10,14,17	2,15,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	5,7,10,14,16,18	2,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	5,7,10,18	2,13,18	2^{-1}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	5,7,10,16,17	2,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	5,7,10	2,13,15	2^{-1}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	5,7,10,16,17,18	2,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	5,7,10,14,17	2,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	5,7,10,14,16,18	2,13,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	5,7,10,14,17,18	2,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	5,7,10,14,16	2,13,15	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	5,7,10,12,17,18	2,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	5,7,10,12,16	2	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	5,7,10,12,17	2,15,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	5,7,10,12,16,18	2,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	5,7,10,12,14	2	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	5,7,10,12,14,16,17,18	2,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	5,7,10,12,14,18	2,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	5,7,10,12,14,16,17	2,15,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	5,7,10,12,17,18	2,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	5,7,10,12,16,18	2,13,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	5,7,10,12,17,18	2,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	5,7,10,12,16	2,13,15	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	5,7,10,12,14,18	2,13,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	5,7,10,12,14,16,17	2,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	5,7,10,12,14	2,13,15	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	5,7,10,12,14,16,17,18	2,13,15,17,18	$2^{-17.5}$

Table 0.596 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	5,7,10,18	2,11,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	5,7,10,16,17	2,11,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	5,7,10	2,11,15	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	5,7,10,16,17,18	2,11,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	5,7,10,14,17	2,11,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	5,7,10,14,16,18	2,11,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	5,7,10,14,17,18	2,11,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	5,7,10,14,16	2,11,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	5,7,10	2,11,13	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	5,7,10,16,17,18	2,11,13,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	5,7,10,18	2,11,13,15,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	5,7,10,16,17	2,11,13,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	5,7,10,14,17,18	2,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	5,7,10,14,16	2,11,13	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	5,7,10,14,17	2,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	5,7,10,14,16,18	2,11,13,15,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	5,7,10,12,17	2,11,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	5,7,10,12,16,18	2,11,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	5,7,10,12,17,18	2,11,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	5,7,10,12,16	2,11,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	5,7,10,12,14,18	2,11,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	5,7,10,12,14,16,17	2,11,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	5,7,10,12,14	2,11,15	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	5,7,10,12,14,16,17,18	2,11,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	5,7,10,12,17,18	2,11,13,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	5,7,10,12,16	2,11,13	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	5,7,10,12,17	2,11,13,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	5,7,10,12,16,18	2,11,13,15,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	5,7,10,12,14	2,11,13	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	5,7,10,12,14,16,17,18	2,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	5,7,10,12,14,18	2,11,13,15,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	5,7,10,12,14,16,17	2,11,13,15,17	$2^{-17.5}$

Table 0.597 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	5,7,17	2,9,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	5,7,16,18	2,9,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	5,7,17,18	2,9,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	5,7,16	2,9,15	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	5,7,14,18	2,9,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	5,7,14,16,17	2,9,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	5,7,14	2,9,15	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	5,7,14,16,17,18	2,9,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	5,7,17,18	2,9,13,17,18	2^{-1}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	5,7,16	2,9,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	5,7,17	2,9,13,15,17	2^{-1}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	5,7,16,18	2,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	5,7,14	2,9,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	5,7,14,16,17,18	2,9,13,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	5,7,14,18	2,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	5,7,14,16,17	2,9,13,15,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	5,7,12,18	2,9,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	5,7,12,16,17	2,9,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	5,7,12	2,9,15	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	5,7,12,16,17,18	2,9,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	5,7,12,14,17	2,9,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	5,7,12,14,16,18	2,9,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	5,7,12,14,17,18	2,9,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	5,7,12,14,16	2,9,15	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	5,7,12	2,9,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	5,7,12,16,17,18	2,9,13,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	5,7,12,18	2,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	5,7,12,16,17	2,9,13,15,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	5,7,12,14,17,18	2,9,13,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	5,7,12,14,16	2,9,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	5,7,12,14,17	2,9,13,15,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	5,7,12,14,16,18	2,9,13,15,18	$2^{-17.5}$

Table 0.598 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	5,7,17,18	2,9,11,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	5,7,16	2,9,11	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	5,7,17	2,9,11,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	5,7,16,18	2,9,11,15,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	5,7,14	2,9,11	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	5,7,14,16,17,18	2,9,11,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	5,7,14,18	2,9,11,15,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	5,7,14,16,17	2,9,11,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	5,7,17	2,9,11,13,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	5,7,16,18	2,9,11,13,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	5,7,17,18	2,9,11,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	5,7,16	2,9,11,13,15	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	5,7,14,18	2,9,11,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	5,7,14,16,17	2,9,11,13,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	5,7,14	2,9,11,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	5,7,14,16,17,18	2,9,11,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	5,7,12	2,9,11	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	5,7,12,16,17,18	2,9,11,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	5,7,12,18	2,9,11,15,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	5,7,12,16,17	2,9,11,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	5,7,12,14,17,18	2,9,11,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	5,7,12,14,16	2,9,11	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	5,7,12,14,17	2,9,11,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	5,7,12,14,16,18	2,9,11,15,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	5,7,12,18	2,9,11,13,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	5,7,12,16,17	2,9,11,13,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	5,7,12	2,9,11,13,15	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	5,7,12,16,17,18	2,9,11,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	5,7,12,14,17	2,9,11,13,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	5,7,12,14,16,18	2,9,11,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	5,7,12,14,17,18	2,9,11,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	5,7,12,14,16	2,9,11,13,15	$2^{-17.5}$

Table 0.599 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	5,7,10,18	2,9,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	5,7,10,16,17	2,9,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	5,7,10	2,9,15	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	5,7,10,16,17,18	2,9,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	5,7,10,14,17	2,9,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	5,7,10,14,16,18	2,9,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	5,7,10,14,17,18	2,9,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	5,7,10,14,16	2,9,15	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	5,7,10	2,9,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	5,7,10,16,17,18	2,9,13,17,18	2^{-34}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	5,7,10,18	2,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	5,7,10,16,17	2,9,13,15,17	2^{-34}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	5,7,10,14,17,18	2,9,13,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	5,7,10,14,16	2,9,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	5,7,10,14,17	2,9,13,15,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	5,7,10,14,16,18	2,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	5,7,10,12,17	2,9,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	5,7,10,12,16,18	2,9,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	5,7,10,12,17,18	2,9,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	5,7,10,12,16	2,9,15	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	5,7,10,12,14,18	2,9,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	5,7,10,12,14,16,17	2,9,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	5,7,10,12,14	2,9,15	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	5,7,10,12,14,16,17,18	2,9,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	5,7,10,12,17,18	2,9,13,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	5,7,10,12,16	2,9,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	5,7,10,12,17	2,9,13,15,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	5,7,10,12,16,18	2,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	5,7,10,12,14	2,9,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	5,7,10,12,14,16,17,18	2,9,13,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	5,7,10,12,14,18	2,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	5,7,10,12,14,16,17	2,9,13,15,17	2^{-23}

Table 0.600 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	5,7,10	2,9,11	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	5,7,10,16,17,18	2,9,11,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	5,7,10,18	2,9,11,15,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	5,7,10,16,17	2,9,11,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	5,7,10,14,17,18	2,9,11,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	5,7,10,14,16	2,9,11	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	5,7,10,14,17	2,9,11,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	5,7,10,14,16,18	2,9,11,15,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	5,7,10,18	2,9,11,13,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	5,7,10,16,17	2,9,11,13,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	5,7,10	2,9,11,13,15	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	5,7,10,16,17,18	2,9,11,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	5,7,10,14,17	2,9,11,13,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	5,7,10,14,16,18	2,9,11,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	5,7,10,14,17,18	2,9,11,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	5,7,10,14,16	2,9,11,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	5,7,10,12,17,18	2,9,11,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	5,7,10,12,16	2,9,11	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	5,7,10,12,17	2,9,11,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	5,7,10,12,16,18	2,9,11,15,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	5,7,10,12,14	2,9,11	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	5,7,10,12,14,16,17,18	2,9,11,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	5,7,10,12,14,18	2,9,11,15,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	5,7,10,12,14,16,17	2,9,11,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	5,7,10,12,17	2,9,11,13,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	5,7,10,12,16,18	2,9,11,13,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	5,7,10,12,17,18	2,9,11,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	5,7,10,12,16	2,9,11,13,15	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	5,7,10,12,14,18	2,9,11,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	5,7,10,12,14,16,17	2,9,11,13,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	5,7,10,12,14	2,9,11,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	5,7,10,12,14,16,17,18	2,9,11,13,15,17,18	2^{-23}

Table 0.601 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	5,7	2,8	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	5,7,16,17,18	2,8,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	5,7,18	2,8,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	5,7,16,17	2,8,15,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	5,7,14,17,18	2,8,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	5,7,14,16	2,8	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	5,7,14,17	2,8,15,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	5,7,14,16,18	2,8,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	5,7,18	2,8,13,18	2^{-34}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	5,7,16,17	2,8,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	5,7	2,8,13,15	2^{-34}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	5,7,16,17,18	2,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	5,7,14,17	2,8,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	5,7,14,16,18	2,8,13,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	5,7,14,17,18	2,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	5,7,14,16	2,8,13,15	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	5,7,12,17,18	2,8,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	5,7,12,16	2,8	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	5,7,12,17	2,8,15,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	5,7,12,16,18	2,8,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	5,7,12,14	2,8	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	5,7,12,14,16,17,18	2,8,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	5,7,12,14,18	2,8,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	5,7,12,14,16,17	2,8,15,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	5,7,12,17	2,8,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	5,7,12,16,18	2,8,13,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	5,7,12,17,18	2,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	5,7,12,16	2,8,13,15	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	5,7,12,14,18	2,8,13,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	5,7,12,14,16,17	2,8,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	5,7,12,14	2,8,13,15	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	5,7,12,14,16,17,18	2,8,13,15,17,18	$2^{-17.5}$

Table 0.602 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	5,7,18	2,8,11,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	5,7,16,17	2,8,11,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	5,7	2,8,11,15	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	5,7,16,17,18	2,8,11,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	5,7,14,17	2,8,11,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	5,7,14,16,18	2,8,11,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	5,7,14,17,18	2,8,11,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	5,7,14,16	2,8,11,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	5,7	2,8,11,13	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	5,7,16,17,18	2,8,11,13,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	5,7,18	2,8,11,13,15,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	5,7,16,17	2,8,11,13,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	5,7,14,17,18	2,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	5,7,14,16	2,8,11,13	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	5,7,14,17	2,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	5,7,14,16,18	2,8,11,13,15,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	5,7,12,17	2,8,11,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	5,7,12,16,18	2,8,11,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	5,7,12,17,18	2,8,11,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	5,7,12,16	2,8,11,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	5,7,12,14,18	2,8,11,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	5,7,12,14,16,17	2,8,11,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	5,7,12,14	2,8,11,15	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	5,7,12,14,16,17,18	2,8,11,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	5,7,12,17,18	2,8,11,13,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	5,7,12,16	2,8,11,13	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	5,7,12,17	2,8,11,13,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	5,7,12,16,18	2,8,11,13,15,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	5,7,12,14	2,8,11,13	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	5,7,12,14,16,17,18	2,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	5,7,12,14,18	2,8,11,13,15,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	5,7,12,14,16,17	2,8,11,13,15,17	$2^{-17.5}$

Table 0.603 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	5,7,10,17,18	2,8,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	5,7,10,16	2,8	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	5,7,10,17	2,8,15,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	5,7,10,16,18	2,8,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	5,7,10,14	2,8	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	5,7,10,14,16,17,18	2,8,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	5,7,10,14,18	2,8,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	5,7,10,14,16,17	2,8,15,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	5,7,10,17	2,8,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	5,7,10,16,18	2,8,13,18	2^{-1}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	5,7,10,17,18	2,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	5,7,10,16	2,8,13,15	2^{-1}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	5,7,10,14,18	2,8,13,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	5,7,10,14,16,17	2,8,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	5,7,10,14	2,8,13,15	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	5,7,10,14,16,17,18	2,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	5,7,10,12	2,8	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	5,7,10,12,16,17,18	2,8,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	5,7,10,12,18	2,8,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	5,7,10,12,16,17	2,8,15,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	5,7,10,12,14,17,18	2,8,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	5,7,10,12,14,16	2,8	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	5,7,10,12,14,17	2,8,15,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	5,7,10,12,14,16,18	2,8,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	5,7,10,12,18	2,8,13,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	5,7,10,12,16,17	2,8,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	5,7,10,12	2,8,13,15	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	5,7,10,12,16,17,18	2,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	5,7,10,12,14,17	2,8,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	5,7,10,12,14,16,18	2,8,13,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	5,7,10,12,14,17,18	2,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	5,7,10,12,14,16	2,8,13,15	2^{-12}

Table 0.604 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	5,7,10,17	2,8,11,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	5,7,10,16,18	2,8,11,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	5,7,10,17,18	2,8,11,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	5,7,10,16	2,8,11,15	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	5,7,10,14,18	2,8,11,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	5,7,10,14,16,17	2,8,11,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	5,7,10,14	2,8,11,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	5,7,10,14,16,17,18	2,8,11,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	5,7,10,17,18	2,8,11,13,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	5,7,10,16	2,8,11,13	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	5,7,10,17	2,8,11,13,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	5,7,10,16,18	2,8,11,13,15,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	5,7,10,14	2,8,11,13	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	5,7,10,14,16,17,18	2,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	5,7,10,14,18	2,8,11,13,15,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	5,7,10,14,16,17	2,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	5,7,10,12,18	2,8,11,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	5,7,10,12,16,17	2,8,11,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	5,7,10,12	2,8,11,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	5,7,10,12,16,17,18	2,8,11,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	5,7,10,12,14,17	2,8,11,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	5,7,10,12,14,16,18	2,8,11,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	5,7,10,12,14,17,18	2,8,11,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	5,7,10,12,14,16	2,8,11,15	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	5,7,10,12	2,8,11,13	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	5,7,10,12,16,17,18	2,8,11,13,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	5,7,10,12,18	2,8,11,13,15,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	5,7,10,12,16,17	2,8,11,13,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	5,7,10,12,14,17,18	2,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	5,7,10,12,14,16	2,8,11,13	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	5,7,10,12,14,17	2,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	5,7,10,12,14,16,18	2,8,11,13,15,18	2^{-12}

Table 0.605 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	5,7,18	2,8,9,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	5,7,16,17	2,8,9,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	5,7	2,8,9,15	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	5,7,16,17,18	2,8,9,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	5,7,14,17	2,8,9,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	5,7,14,16,18	2,8,9,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	5,7,14,17,18	2,8,9,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	5,7,14,16	2,8,9,15	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	5,7	2,8,9,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	5,7,16,17,18	2,8,9,13,17,18	2^{-1}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	5,7,18	2,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	5,7,16,17	2,8,9,13,15,17	2^{-1}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	5,7,14,17,18	2,8,9,13,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	5,7,14,16	2,8,9,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	5,7,14,17	2,8,9,13,15,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	5,7,14,16,18	2,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	5,7,12,17	2,8,9,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	5,7,12,16,18	2,8,9,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	5,7,12,17,18	2,8,9,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	5,7,12,16	2,8,9,15	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	5,7,12,14,18	2,8,9,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	5,7,12,14,16,17	2,8,9,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	5,7,12,14	2,8,9,15	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	5,7,12,14,16,17,18	2,8,9,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	5,7,12,17,18	2,8,9,13,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	5,7,12,16	2,8,9,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	5,7,12,17	2,8,9,13,15,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	5,7,12,16,18	2,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	5,7,12,14	2,8,9,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	5,7,12,14,16,17,18	2,8,9,13,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	5,7,12,14,18	2,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	5,7,12,14,16,17	2,8,9,13,15,17	2^{-12}

Table 0.606 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	5,7	2,8,9,11	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	5,7,16,17,18	2,8,9,11,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	5,7,18	2,8,9,11,15,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	5,7,16,17	2,8,9,11,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	5,7,14,17,18	2,8,9,11,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	5,7,14,16	2,8,9,11	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	5,7,14,17	2,8,9,11,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	5,7,14,16,18	2,8,9,11,15,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	5,7,18	2,8,9,11,13,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	5,7,16,17	2,8,9,11,13,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	5,7	2,8,9,11,13,15	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	5,7,16,17,18	2,8,9,11,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	5,7,14,17	2,8,9,11,13,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	5,7,14,16,18	2,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	5,7,14,17,18	2,8,9,11,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	5,7,14,16	2,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	5,7,12,17,18	2,8,9,11,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	5,7,12,16	2,8,9,11	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	5,7,12,17	2,8,9,11,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	5,7,12,16,18	2,8,9,11,15,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	5,7,12,14	2,8,9,11	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	5,7,12,14,16,17,18	2,8,9,11,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	5,7,12,14,18	2,8,9,11,15,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	5,7,12,14,16,17	2,8,9,11,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	5,7,12,17	2,8,9,11,13,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	5,7,12,16,18	2,8,9,11,13,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	5,7,12,17,18	2,8,9,11,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	5,7,12,16	2,8,9,11,13,15	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	5,7,12,14,18	2,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	5,7,12,14,16,17	2,8,9,11,13,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	5,7,12,14	2,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	5,7,12,14,16,17,18	2,8,9,11,13,15,17,18	2^{-12}

Table 0.607 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	5,7,10,17	2,8,9,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	5,7,10,16,18	2,8,9,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	5,7,10,17,18	2,8,9,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	5,7,10,16	2,8,9,15	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	5,7,10,14,18	2,8,9,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	5,7,10,14,16,17	2,8,9,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	5,7,10,14	2,8,9,15	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	5,7,10,14,16,17,18	2,8,9,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	5,7,10,17,18	2,8,9,13,17,18	2^{-34}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	5,7,10,16	2,8,9,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	5,7,10,17	2,8,9,13,15,17	2^{-34}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	5,7,10,16,18	2,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	5,7,10,14	2,8,9,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	5,7,10,14,16,17,18	2,8,9,13,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	5,7,10,14,18	2,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	5,7,10,14,16,17	2,8,9,13,15,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	5,7,10,12,18	2,8,9,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	5,7,10,12,16,17	2,8,9,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	5,7,10,12	2,8,9,15	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	5,7,10,12,16,17,18	2,8,9,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	5,7,10,12,14,17	2,8,9,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	5,7,10,12,14,16,18	2,8,9,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	5,7,10,12,14,17,18	2,8,9,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	5,7,10,12,14,16	2,8,9,15	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	5,7,10,12	2,8,9,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	5,7,10,12,16,17,18	2,8,9,13,17,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	5,7,10,12,18	2,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	5,7,10,12,16,17	2,8,9,13,15,17	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	5,7,10,12,14,17,18	2,8,9,13,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	5,7,10,12,14,16	2,8,9,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	5,7,10,12,14,17	2,8,9,13,15,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	5,7,10,12,14,16,18	2,8,9,13,15,18	$2^{-17.5}$

Table 0.608 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	5,7,10,17,18	2,8,9,11,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	5,7,10,16	2,8,9,11	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	5,7,10,17	2,8,9,11,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	5,7,10,16,18	2,8,9,11,15,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	5,7,10,14	2,8,9,11	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	5,7,10,14,16,17,18	2,8,9,11,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	5,7,10,14,18	2,8,9,11,15,18	2^{-12}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	5,7,10,14,16,17	2,8,9,11,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	5,7,10,17	2,8,9,11,13,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	5,7,10,16,18	2,8,9,11,13,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	5,7,10,17,18	2,8,9,11,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	5,7,10,16	2,8,9,11,13,15	$2^{-6.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	5,7,10,14,18	2,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	5,7,10,14,16,17	2,8,9,11,13,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	5,7,10,14	2,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	5,7,10,14,16,17,18	2,8,9,11,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	5,7,10,12	2,8,9,11	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	5,7,10,12,16,17,18	2,8,9,11,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	5,7,10,12,18	2,8,9,11,15,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	5,7,10,12,16,17	2,8,9,11,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	5,7,10,12,14,17,18	2,8,9,11,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	5,7,10,12,14,16	2,8,9,11	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	5,7,10,12,14,17	2,8,9,11,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	5,7,10,12,14,16,18	2,8,9,11,15,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	5,7,10,12,18	2,8,9,11,13,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	5,7,10,12,16,17	2,8,9,11,13,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	5,7,10,12	2,8,9,11,13,15	$2^{-28.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	5,7,10,12,16,17,18	2,8,9,11,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	5,7,10,12,14,17	2,8,9,11,13,17	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	5,7,10,12,14,16,18	2,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	5,7,10,12,14,17,18	2,8,9,11,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	5,7,10,12,14,16	2,8,9,11,13,15	$2^{-17.5}$

Table 0.609 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	5,18	2,6,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	5,16,17	2,6,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	5	2,6,15	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	5,16,17,18	2,6,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	5,14,17	2,6,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	5,14,16,18	2,6,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	5,14,17,18	2,6,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	5,14,16	2,6,15	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	5	2,6,13	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	5,16,17,18	2,6,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	5,18	2,6,13,15,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	5,16,17	2,6,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	5,14,17,18	2,6,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	5,14,16	2,6,13	2^{-34}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	5,14,17	2,6,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	5,14,16,18	2,6,13,15,18	2^{-34}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	5,12,17	2,6,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	5,12,16,18	2,6,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	5,12,17,18	2,6,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	5,12,16	2,6,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	5,12,14,18	2,6,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	5,12,14,16,17	2,6,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	5,12,14	2,6,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	5,12,14,16,17,18	2,6,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	5,12,17,18	2,6,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	5,12,16	2,6,13	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	5,12,17	2,6,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	5,12,16,18	2,6,13,15,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	5,12,14	2,6,13	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	5,12,14,16,17,18	2,6,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	5,12,14,18	2,6,13,15,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	5,12,14,16,17	2,6,13,15,17	$2^{-17.5}$

Table 0.610 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	5	2,6,11	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	5,16,17,18	2,6,11,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	5,18	2,6,11,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	5,16,17	2,6,11,15,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	5,14,17,18	2,6,11,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	5,14,16	2,6,11	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	5,14,17	2,6,11,15,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	5,14,16,18	2,6,11,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	5,18	2,6,11,13,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	5,16,17	2,6,11,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	5	2,6,11,13,15	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	5,16,17,18	2,6,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	5,14,17	2,6,11,13,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	5,14,16,18	2,6,11,13,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	5,14,17,18	2,6,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	5,14,16	2,6,11,13,15	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	5,12,17,18	2,6,11,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	5,12,16	2,6,11	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	5,12,17	2,6,11,15,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	5,12,16,18	2,6,11,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	5,12,14	2,6,11	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	5,12,14,16,17,18	2,6,11,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	5,12,14,18	2,6,11,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	5,12,14,16,17	2,6,11,15,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	5,12,17	2,6,11,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	5,12,16,18	2,6,11,13,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	5,12,17,18	2,6,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	5,12,16	2,6,11,13,15	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	5,12,14,18	2,6,11,13,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	5,12,14,16,17	2,6,11,13,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	5,12,14	2,6,11,13,15	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	5,12,14,16,17,18	2,6,11,13,15,17,18	$2^{-28.5}$

Table 0.611 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(2)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	5,10,17	2,6,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	5,10,16,18	2,6,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	5,10,17,18	2,6,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	5,10,16	2,6,15	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	5,10,14,18	2,6,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	5,10,14,16,17	2,6,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	5,10,14	2,6,15	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	5,10,14,16,17,18	2,6,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	5,10,17,18	2,6,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	5,10,16	2,6,13	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	5,10,17	2,6,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	5,10,16,18	2,6,13,15,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	5,10,14	2,6,13	2^{-1}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	5,10,14,16,17,18	2,6,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	5,10,14,18	2,6,13,15,18	2^{-1}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	5,10,14,16,17	2,6,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	5,10,12,18	2,6,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	5,10,12,16,17	2,6,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	5,10,12	2,6,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	5,10,12,16,17,18	2,6,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	5,10,12,14,17	2,6,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	5,10,12,14,16,18	2,6,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	5,10,12,14,17,18	2,6,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	5,10,12,14,16	2,6,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	5,10,12	2,6,13	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	5,10,12,16,17,18	2,6,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	5,10,12,18	2,6,13,15,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	5,10,12,16,17	2,6,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	5,10,12,14,17,18	2,6,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	5,10,12,14,16	2,6,13	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	5,10,12,14,17	2,6,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	5,10,12,14,16,18	2,6,13,15,18	2^{-23}

Table 0.612 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	5,10,17,18	2,6,11,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	5,10,16	2,6,11	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	5,10,17	2,6,11,15,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	5,10,16,18	2,6,11,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	5,10,14	2,6,11	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	5,10,14,16,17,18	2,6,11,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	5,10,14,18	2,6,11,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	5,10,14,16,17	2,6,11,15,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	5,10,17	2,6,11,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	5,10,16,18	2,6,11,13,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	5,10,17,18	2,6,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	5,10,16	2,6,11,13,15	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	5,10,14,18	2,6,11,13,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	5,10,14,16,17	2,6,11,13,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	5,10,14	2,6,11,13,15	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	5,10,14,16,17,18	2,6,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	5,10,12	2,6,11	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	5,10,12,16,17,18	2,6,11,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	5,10,12,18	2,6,11,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	5,10,12,16,17	2,6,11,15,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	5,10,12,14,17,18	2,6,11,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	5,10,12,14,16	2,6,11	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	5,10,12,14,17	2,6,11,15,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	5,10,12,14,16,18	2,6,11,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	5,10,12,18	2,6,11,13,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	5,10,12,16,17	2,6,11,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	5,10,12	2,6,11,13,15	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	5,10,12,16,17,18	2,6,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	5,10,12,14,17	2,6,11,13,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	5,10,12,14,16,18	2,6,11,13,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	5,10,12,14,17,18	2,6,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	5,10,12,14,16	2,6,11,13,15	2^{-12}

Table 0.613 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	5	2,6,9	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	5,16,17,18	2,6,9,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	5,18	2,6,9,15,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	5,16,17	2,6,9,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	5,14,17,18	2,6,9,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	5,14,16	2,6,9	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	5,14,17	2,6,9,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	5,14,16,18	2,6,9,15,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	5,18	2,6,9,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	5,16,17	2,6,9,13,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	5	2,6,9,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	5,16,17,18	2,6,9,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	5,14,17	2,6,9,13,17	2^{-1}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	5,14,16,18	2,6,9,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	5,14,17,18	2,6,9,13,15,17,18	2^{-1}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	5,14,16	2,6,9,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	5,12,17,18	2,6,9,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	5,12,16	2,6,9	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	5,12,17	2,6,9,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	5,12,16,18	2,6,9,15,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	5,12,14	2,6,9	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	5,12,14,16,17,18	2,6,9,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	5,12,14,18	2,6,9,15,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	5,12,14,16,17	2,6,9,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	5,12,17	2,6,9,13,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	5,12,16,18	2,6,9,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	5,12,17,18	2,6,9,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	5,12,16	2,6,9,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	5,12,14,18	2,6,9,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	5,12,14,16,17	2,6,9,13,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	5,12,14	2,6,9,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	5,12,14,16,17,18	2,6,9,13,15,17,18	2^{-23}

Table 0.614 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	5,18	2,6,9,11,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	5,16,17	2,6,9,11,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	5	2,6,9,11,15	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	5,16,17,18	2,6,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	5,14,17	2,6,9,11,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	5,14,16,18	2,6,9,11,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	5,14,17,18	2,6,9,11,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	5,14,16	2,6,9,11,15	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	5	2,6,9,11,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	5,16,17,18	2,6,9,11,13,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	5,18	2,6,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	5,16,17	2,6,9,11,13,15,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	5,14,17,18	2,6,9,11,13,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	5,14,16	2,6,9,11,13	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	5,14,17	2,6,9,11,13,15,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	5,14,16,18	2,6,9,11,13,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	5,12,17	2,6,9,11,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	5,12,16,18	2,6,9,11,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	5,12,17,18	2,6,9,11,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	5,12,16	2,6,9,11,15	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	5,12,14,18	2,6,9,11,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	5,12,14,16,17	2,6,9,11,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	5,12,14	2,6,9,11,15	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	5,12,14,16,17,18	2,6,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	5,12,17,18	2,6,9,11,13,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	5,12,16	2,6,9,11,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	5,12,17	2,6,9,11,13,15,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	5,12,16,18	2,6,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	5,12,14	2,6,9,11,13	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	5,12,14,16,17,18	2,6,9,11,13,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	5,12,14,18	2,6,9,11,13,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	5,12,14,16,17	2,6,9,11,13,15,17	2^{-12}

Table 0.615 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	5,10,17,18	2,6,9,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	5,10,16	2,6,9	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	5,10,17	2,6,9,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	5,10,16,18	2,6,9,15,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	5,10,14	2,6,9	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	5,10,14,16,17,18	2,6,9,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	5,10,14,18	2,6,9,15,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	5,10,14,16,17	2,6,9,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	5,10,17	2,6,9,13,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	5,10,16,18	2,6,9,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	5,10,17,18	2,6,9,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	5,10,16	2,6,9,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	5,10,14,18	2,6,9,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	5,10,14,16,17	2,6,9,13,17	2^{-34}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	5,10,14	2,6,9,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	5,10,14,16,17,18	2,6,9,13,15,17,18	2^{-34}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	5,10,12	2,6,9	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	5,10,12,16,17,18	2,6,9,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	5,10,12,18	2,6,9,15,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	5,10,12,16,17	2,6,9,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	5,10,12,14,17,18	2,6,9,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	5,10,12,14,16	2,6,9	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	5,10,12,14,17	2,6,9,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	5,10,12,14,16,18	2,6,9,15,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	5,10,12,18	2,6,9,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	5,10,12,16,17	2,6,9,13,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	5,10,12	2,6,9,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	5,10,12,16,17,18	2,6,9,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	5,10,12,14,17	2,6,9,13,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	5,10,12,14,16,18	2,6,9,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	5,10,12,14,17,18	2,6,9,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	5,10,12,14,16	2,6,9,13,15	$2^{-17.5}$

Table 0.616 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	5,10,17	2,6,9,11,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	5,10,16,18	2,6,9,11,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	5,10,17,18	2,6,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	5,10,16	2,6,9,11,15	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	5,10,14,18	2,6,9,11,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	5,10,14,16,17	2,6,9,11,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	5,10,14	2,6,9,11,15	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	5,10,14,16,17,18	2,6,9,11,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	5,10,17,18	2,6,9,11,13,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	5,10,16	2,6,9,11,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	5,10,17	2,6,9,11,13,15,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	5,10,16,18	2,6,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	5,10,14	2,6,9,11,13	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	5,10,14,16,17,18	2,6,9,11,13,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	5,10,14,18	2,6,9,11,13,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	5,10,14,16,17	2,6,9,11,13,15,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	5,10,12,18	2,6,9,11,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	5,10,12,16,17	2,6,9,11,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	5,10,12	2,6,9,11,15	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	5,10,12,16,17,18	2,6,9,11,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	5,10,12,14,17	2,6,9,11,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	5,10,12,14,16,18	2,6,9,11,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	5,10,12,14,17,18	2,6,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	5,10,12,14,16	2,6,9,11,15	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	5,10,12	2,6,9,11,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	5,10,12,16,17,18	2,6,9,11,13,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	5,10,12,18	2,6,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	5,10,12,16,17	2,6,9,11,13,15,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	5,10,12,14,17,18	2,6,9,11,13,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	5,10,12,14,16	2,6,9,11,13	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	5,10,12,14,17	2,6,9,11,13,15,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	5,10,12,14,16,18	2,6,9,11,13,15,18	$2^{-28.5}$

Table 0.617 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	5,17	2,6,8,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	5,16,18	2,6,8,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	5,17,18	2,6,8,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	5,16	2,6,8,15	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	5,14,18	2,6,8,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	5,14,16,17	2,6,8,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	5,14	2,6,8,15	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	5,14,16,17,18	2,6,8,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	5,17,18	2,6,8,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	5,16	2,6,8,13	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	5,17	2,6,8,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	5,16,18	2,6,8,13,15,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	5,14	2,6,8,13	2^{-34}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	5,14,16,17,18	2,6,8,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	5,14,18	2,6,8,13,15,18	2^{-34}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	5,14,16,17	2,6,8,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	5,12,18	2,6,8,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	5,12,16,17	2,6,8,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	5,12	2,6,8,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	5,12,16,17,18	2,6,8,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	5,12,14,17	2,6,8,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	5,12,14,16,18	2,6,8,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	5,12,14,17,18	2,6,8,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	5,12,14,16	2,6,8,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	5,12	2,6,8,13	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	5,12,16,17,18	2,6,8,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	5,12,18	2,6,8,13,15,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	5,12,16,17	2,6,8,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	5,12,14,17,18	2,6,8,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	5,12,14,16	2,6,8,13	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	5,12,14,17	2,6,8,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	5,12,14,16,18	2,6,8,13,15,18	2^{-12}

Table 0.618 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	5,17,18	2,6,8,11,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	5,16	2,6,8,11	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	5,17	2,6,8,11,15,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	5,16,18	2,6,8,11,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	5,14	2,6,8,11	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	5,14,16,17,18	2,6,8,11,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	5,14,18	2,6,8,11,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	5,14,16,17	2,6,8,11,15,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	5,17	2,6,8,11,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	5,16,18	2,6,8,11,13,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	5,17,18	2,6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	5,16	2,6,8,11,13,15	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	5,14,18	2,6,8,11,13,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	5,14,16,17	2,6,8,11,13,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	5,14	2,6,8,11,13,15	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	5,14,16,17,18	2,6,8,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	5,12	2,6,8,11	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	5,12,16,17,18	2,6,8,11,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	5,12,18	2,6,8,11,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	5,12,16,17	2,6,8,11,15,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	5,12,14,17,18	2,6,8,11,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	5,12,14,16	2,6,8,11	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	5,12,14,17	2,6,8,11,15,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	5,12,14,16,18	2,6,8,11,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	5,12,18	2,6,8,11,13,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	5,12,16,17	2,6,8,11,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	5,12	2,6,8,11,13,15	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	5,12,16,17,18	2,6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	5,12,14,17	2,6,8,11,13,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	5,12,14,16,18	2,6,8,11,13,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	5,12,14,17,18	2,6,8,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	5,12,14,16	2,6,8,11,13,15	2^{-23}

Table 0.619 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	5,10,18	2,6,8,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	5,10,16,17	2,6,8,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	5,10	2,6,8,15	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	5,10,16,17,18	2,6,8,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	5,10,14,17	2,6,8,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	5,10,14,16,18	2,6,8,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	5,10,14,17,18	2,6,8,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	5,10,14,16	2,6,8,15	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	5,10	2,6,8,13	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	5,10,16,17,18	2,6,8,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	5,10,18	2,6,8,13,15,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	5,10,16,17	2,6,8,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	5,10,14,17,18	2,6,8,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	5,10,14,16	2,6,8,13	2^{-1}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	5,10,14,17	2,6,8,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	5,10,14,16,18	2,6,8,13,15,18	2^{-1}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	5,10,12,17	2,6,8,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	5,10,12,16,18	2,6,8,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	5,10,12,17,18	2,6,8,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	5,10,12,16	2,6,8,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	5,10,12,14,18	2,6,8,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	5,10,12,14,16,17	2,6,8,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	5,10,12,14	2,6,8,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	5,10,12,14,16,17,18	2,6,8,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	5,10,12,17,18	2,6,8,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	5,10,12,16	2,6,8,13	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	5,10,12,17	2,6,8,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	5,10,12,16,18	2,6,8,13,15,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	5,10,12,14	2,6,8,13	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	5,10,12,14,16,17,18	2,6,8,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	5,10,12,14,18	2,6,8,13,15,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	5,10,12,14,16,17	2,6,8,13,15,17	$2^{-17.5}$

Table 0.620 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	5,10	2,6,8,11	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	5,10,16,17,18	2,6,8,11,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	5,10,18	2,6,8,11,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	5,10,16,17	2,6,8,11,15,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	5,10,14,17,18	2,6,8,11,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	5,10,14,16	2,6,8,11	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	5,10,14,17	2,6,8,11,15,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	5,10,14,16,18	2,6,8,11,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	5,10,18	2,6,8,11,13,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	5,10,16,17	2,6,8,11,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	5,10	2,6,8,11,13,15	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	5,10,16,17,18	2,6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	5,10,14,17	2,6,8,11,13,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	5,10,14,16,18	2,6,8,11,13,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	5,10,14,17,18	2,6,8,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	5,10,14,16	2,6,8,11,13,15	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	5,10,12,17,18	2,6,8,11,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	5,10,12,16	2,6,8,11	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	5,10,12,17	2,6,8,11,15,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	5,10,12,16,18	2,6,8,11,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	5,10,12,14	2,6,8,11	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	5,10,12,14,16,17,18	2,6,8,11,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	5,10,12,14,18	2,6,8,11,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	5,10,12,14,16,17	2,6,8,11,15,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	5,10,12,17	2,6,8,11,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	5,10,12,16,18	2,6,8,11,13,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	5,10,12,17,18	2,6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	5,10,12,16	2,6,8,11,13,15	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	5,10,12,14,18	2,6,8,11,13,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	5,10,12,14,16,17	2,6,8,11,13,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	5,10,12,14	2,6,8,11,13,15	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	5,10,12,14,16,17,18	2,6,8,11,13,15,17,18	$2^{-6.5}$

Table 0.621 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	5,17,18	2,6,8,9,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	5,16	2,6,8,9	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	5,17	2,6,8,9,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	5,16,18	2,6,8,9,15,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	5,14	2,6,8,9	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	5,14,16,17,18	2,6,8,9,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	5,14,18	2,6,8,9,15,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	5,14,16,17	2,6,8,9,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	5,17	2,6,8,9,13,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	5,16,18	2,6,8,9,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	5,17,18	2,6,8,9,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	5,16	2,6,8,9,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	5,14,18	2,6,8,9,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	5,14,16,17	2,6,8,9,13,17	2^{-1}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	5,14	2,6,8,9,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	5,14,16,17,18	2,6,8,9,13,15,17,18	2^{-1}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	5,12	2,6,8,9	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	5,12,16,17,18	2,6,8,9,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	5,12,18	2,6,8,9,15,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	5,12,16,17	2,6,8,9,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	5,12,14,17,18	2,6,8,9,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	5,12,14,16	2,6,8,9	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	5,12,14,17	2,6,8,9,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	5,12,14,16,18	2,6,8,9,15,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	5,12,18	2,6,8,9,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	5,12,16,17	2,6,8,9,13,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	5,12	2,6,8,9,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	5,12,16,17,18	2,6,8,9,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	5,12,14,17	2,6,8,9,13,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	5,12,14,16,18	2,6,8,9,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	5,12,14,17,18	2,6,8,9,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	5,12,14,16	2,6,8,9,13,15	$2^{-17.5}$

Table 0.622 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	5,17	2,6,8,9,11,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	5,16,18	2,6,8,9,11,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	5,17,18	2,6,8,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	5,16	2,6,8,9,11,15	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	5,14,18	2,6,8,9,11,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	5,14,16,17	2,6,8,9,11,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	5,14	2,6,8,9,11,15	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	5,14,16,17,18	2,6,8,9,11,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	5,17,18	2,6,8,9,11,13,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	5,16	2,6,8,9,11,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	5,17	2,6,8,9,11,13,15,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	5,16,18	2,6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	5,14	2,6,8,9,11,13	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	5,14,16,17,18	2,6,8,9,11,13,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	5,14,18	2,6,8,9,11,13,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	5,14,16,17	2,6,8,9,11,13,15,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	5,12,18	2,6,8,9,11,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	5,12,16,17	2,6,8,9,11,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	5,12	2,6,8,9,11,15	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	5,12,16,17,18	2,6,8,9,11,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	5,12,14,17	2,6,8,9,11,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	5,12,14,16,18	2,6,8,9,11,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	5,12,14,17,18	2,6,8,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	5,12,14,16	2,6,8,9,11,15	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	5,12	2,6,8,9,11,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	5,12,16,17,18	2,6,8,9,11,13,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	5,12,18	2,6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	5,12,16,17	2,6,8,9,11,13,15,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	5,12,14,17,18	2,6,8,9,11,13,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	5,12,14,16	2,6,8,9,11,13	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	5,12,14,17	2,6,8,9,11,13,15,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	5,12,14,16,18	2,6,8,9,11,13,15,18	$2^{-6.5}$

Table 0.623 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	5,10	2,6,8,9	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	5,10,16,17,18	2,6,8,9,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	5,10,18	2,6,8,9,15,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	5,10,16,17	2,6,8,9,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	5,10,14,17,18	2,6,8,9,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	5,10,14,16	2,6,8,9	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	5,10,14,17	2,6,8,9,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	5,10,14,16,18	2,6,8,9,15,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	5,10,18	2,6,8,9,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	5,10,16,17	2,6,8,9,13,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	5,10	2,6,8,9,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	5,10,16,17,18	2,6,8,9,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	5,10,14,17	2,6,8,9,13,17	2^{-34}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	5,10,14,16,18	2,6,8,9,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	5,10,14,17,18	2,6,8,9,13,15,17,18	2^{-34}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	5,10,14,16	2,6,8,9,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	5,10,12,17,18	2,6,8,9,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	5,10,12,16	2,6,8,9	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	5,10,12,17	2,6,8,9,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	5,10,12,16,18	2,6,8,9,15,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	5,10,12,14	2,6,8,9	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	5,10,12,14,16,17,18	2,6,8,9,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	5,10,12,14,18	2,6,8,9,15,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	5,10,12,14,16,17	2,6,8,9,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	5,10,12,17	2,6,8,9,13,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	5,10,12,16,18	2,6,8,9,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	5,10,12,17,18	2,6,8,9,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	5,10,12,16	2,6,8,9,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	5,10,12,14,18	2,6,8,9,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	5,10,12,14,16,17	2,6,8,9,13,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	5,10,12,14	2,6,8,9,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	5,10,12,14,16,17,18	2,6,8,9,13,15,17,18	2^{-12}

Table 0.624 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	5,10,18	2,6,8,9,11,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	5,10,16,17	2,6,8,9,11,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	5,10	2,6,8,9,11,15	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	5,10,16,17,18	2,6,8,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	5,10,14,17	2,6,8,9,11,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	5,10,14,16,18	2,6,8,9,11,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	5,10,14,17,18	2,6,8,9,11,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	5,10,14,16	2,6,8,9,11,15	2^{-12}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	5,10	2,6,8,9,11,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	5,10,16,17,18	2,6,8,9,11,13,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	5,10,18	2,6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	5,10,16,17	2,6,8,9,11,13,15,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	5,10,14,17,18	2,6,8,9,11,13,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	5,10,14,16	2,6,8,9,11,13	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	5,10,14,17	2,6,8,9,11,13,15,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	5,10,14,16,18	2,6,8,9,11,13,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	5,10,12,17	2,6,8,9,11,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	5,10,12,16,18	2,6,8,9,11,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	5,10,12,17,18	2,6,8,9,11,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	5,10,12,16	2,6,8,9,11,15	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	5,10,12,14,18	2,6,8,9,11,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	5,10,12,14,16,17	2,6,8,9,11,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	5,10,12,14	2,6,8,9,11,15	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	5,10,12,14,16,17,18	2,6,8,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	5,10,12,17,18	2,6,8,9,11,13,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	5,10,12,16	2,6,8,9,11,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	5,10,12,17	2,6,8,9,11,13,15,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	5,10,12,16,18	2,6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	5,10,12,14	2,6,8,9,11,13	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	5,10,12,14,16,17,18	2,6,8,9,11,13,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	5,10,12,14,18	2,6,8,9,11,13,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	5,10,12,14,16,17	2,6,8,9,11,13,15,17	2^{-23}

Table 0.625 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	5,7	2,6	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	5,7,16,17,18	2,6,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	5,7,18	2,6,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	5,7,16,17	2,6,15,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	5,7,14,17,18	2,6,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	5,7,14,16	2,6	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	5,7,14,17	2,6,15,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	5,7,14,16,18	2,6,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	5,7,18	2,6,13,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	5,7,16,17	2,6,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	5,7	2,6,13,15	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	5,7,16,17,18	2,6,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	5,7,14,17	2,6,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	5,7,14,16,18	2,6,13,18	2^{-34}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	5,7,14,17,18	2,6,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	5,7,14,16	2,6,13,15	2^{-34}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	5,7,12,17,18	2,6,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	5,7,12,16	2,6	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	5,7,12,17	2,6,15,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	5,7,12,16,18	2,6,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	5,7,12,14	2,6	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	5,7,12,14,16,17,18	2,6,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	5,7,12,14,18	2,6,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	5,7,12,14,16,17	2,6,15,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	5,7,12,17	2,6,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	5,7,12,16,18	2,6,13,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	5,7,12,17,18	2,6,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	5,7,12,16	2,6,13,15	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	5,7,12,14,18	2,6,13,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	5,7,12,14,16,17	2,6,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	5,7,12,14	2,6,13,15	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	5,7,12,14,16,17,18	2,6,13,15,17,18	$2^{-17.5}$

Table 0.626 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	5,7,18	2,6,11,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	5,7,16,17	2,6,11,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	5,7	2,6,11,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	5,7,16,17,18	2,6,11,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	5,7,14,17	2,6,11,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	5,7,14,16,18	2,6,11,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	5,7,14,17,18	2,6,11,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	5,7,14,16	2,6,11,15	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	5,7	2,6,11,13	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	5,7,16,17,18	2,6,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	5,7,18	2,6,11,13,15,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	5,7,16,17	2,6,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	5,7,14,17,18	2,6,11,13,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	5,7,14,16	2,6,11,13	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	5,7,14,17	2,6,11,13,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	5,7,14,16,18	2,6,11,13,15,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	5,7,12,17	2,6,11,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	5,7,12,16,18	2,6,11,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	5,7,12,17,18	2,6,11,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	5,7,12,16	2,6,11,15	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	5,7,12,14,18	2,6,11,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	5,7,12,14,16,17	2,6,11,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	5,7,12,14	2,6,11,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	5,7,12,14,16,17,18	2,6,11,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	5,7,12,17,18	2,6,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	5,7,12,16	2,6,11,13	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	5,7,12,17	2,6,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	5,7,12,16,18	2,6,11,13,15,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	5,7,12,14	2,6,11,13	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	5,7,12,14,16,17,18	2,6,11,13,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	5,7,12,14,18	2,6,11,13,15,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	5,7,12,14,16,17	2,6,11,13,15,17	$2^{-28.5}$

Table 0.627 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	5,7,10,17,18	2,6,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	5,7,10,16	2,6	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	5,7,10,17	2,6,15,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	5,7,10,16,18	2,6,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	5,7,10,14	2,6	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	5,7,10,14,16,17,18	2,6,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	5,7,10,14,18	2,6,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	5,7,10,14,16,17	2,6,15,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	5,7,10,17	2,6,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	5,7,10,16,18	2,6,13,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	5,7,10,17,18	2,6,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	5,7,10,16	2,6,13,15	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	5,7,10,14,18	2,6,13,18	2^{-1}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	5,7,10,14,16,17	2,6,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	5,7,10,14	2,6,13,15	2^{-1}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	5,7,10,14,16,17,18	2,6,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	5,7,10,12	2,6	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	5,7,10,12,16,17,18	2,6,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	5,7,10,12,18	2,6,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	5,7,10,12,16,17	2,6,15,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	5,7,10,12,14,17,18	2,6,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	5,7,10,12,14,16	2,6	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	5,7,10,12,14,17	2,6,15,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	5,7,10,12,14,16,18	2,6,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	5,7,10,12,18	2,6,13,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	5,7,10,12,16,17	2,6,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	5,7,10,12	2,6,13,15	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	5,7,10,12,16,17,18	2,6,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	5,7,10,12,14,17	2,6,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	5,7,10,12,14,16,18	2,6,13,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	5,7,10,12,14,17,18	2,6,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	5,7,10,12,14,16	2,6,13,15	2^{-23}

Table 0.628 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	5,7,10,17	2,6,11,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	5,7,10,16,18	2,6,11,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	5,7,10,17,18	2,6,11,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	5,7,10,16	2,6,11,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	5,7,10,14,18	2,6,11,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	5,7,10,14,16,17	2,6,11,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	5,7,10,14	2,6,11,15	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	5,7,10,14,16,17,18	2,6,11,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	5,7,10,17,18	2,6,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	5,7,10,16	2,6,11,13	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	5,7,10,17	2,6,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	5,7,10,16,18	2,6,11,13,15,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	5,7,10,14	2,6,11,13	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	5,7,10,14,16,17,18	2,6,11,13,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	5,7,10,14,18	2,6,11,13,15,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	5,7,10,14,16,17	2,6,11,13,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	5,7,10,12,18	2,6,11,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	5,7,10,12,16,17	2,6,11,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	5,7,10,12	2,6,11,15	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	5,7,10,12,16,17,18	2,6,11,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	5,7,10,12,14,17	2,6,11,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	5,7,10,12,14,16,18	2,6,11,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	5,7,10,12,14,17,18	2,6,11,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	5,7,10,12,14,16	2,6,11,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	5,7,10,12	2,6,11,13	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	5,7,10,12,16,17,18	2,6,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	5,7,10,12,18	2,6,11,13,15,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	5,7,10,12,16,17	2,6,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	5,7,10,12,14,17,18	2,6,11,13,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	5,7,10,12,14,16	2,6,11,13	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	5,7,10,12,14,17	2,6,11,13,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	5,7,10,12,14,16,18	2,6,11,13,15,18	2^{-12}

Table 0.629 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	5,7,18	2,6,9,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	5,7,16,17	2,6,9,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	5,7	2,6,9,15	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	5,7,16,17,18	2,6,9,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	5,7,14,17	2,6,9,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	5,7,14,16,18	2,6,9,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	5,7,14,17,18	2,6,9,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	5,7,14,16	2,6,9,15	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	5,7	2,6,9,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	5,7,16,17,18	2,6,9,13,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	5,7,18	2,6,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	5,7,16,17	2,6,9,13,15,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	5,7,14,17,18	2,6,9,13,17,18	2^{-1}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	5,7,14,16	2,6,9,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	5,7,14,17	2,6,9,13,15,17	2^{-1}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	5,7,14,16,18	2,6,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	5,7,12,17	2,6,9,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	5,7,12,16,18	2,6,9,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	5,7,12,17,18	2,6,9,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	5,7,12,16	2,6,9,15	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	5,7,12,14,18	2,6,9,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	5,7,12,14,16,17	2,6,9,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	5,7,12,14	2,6,9,15	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	5,7,12,14,16,17,18	2,6,9,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	5,7,12,17,18	2,6,9,13,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	5,7,12,16	2,6,9,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	5,7,12,17	2,6,9,13,15,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	5,7,12,16,18	2,6,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	5,7,12,14	2,6,9,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	5,7,12,14,16,17,18	2,6,9,13,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	5,7,12,14,18	2,6,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	5,7,12,14,16,17	2,6,9,13,15,17	2^{-23}

Table 0.630 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	5,7	2,6,9,11	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	5,7,16,17,18	2,6,9,11,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	5,7,18	2,6,9,11,15,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	5,7,16,17	2,6,9,11,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	5,7,14,17,18	2,6,9,11,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	5,7,14,16	2,6,9,11	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	5,7,14,17	2,6,9,11,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	5,7,14,16,18	2,6,9,11,15,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	5,7,18	2,6,9,11,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	5,7,16,17	2,6,9,11,13,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	5,7	2,6,9,11,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	5,7,16,17,18	2,6,9,11,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	5,7,14,17	2,6,9,11,13,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	5,7,14,16,18	2,6,9,11,13,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	5,7,14,17,18	2,6,9,11,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	5,7,14,16	2,6,9,11,13,15	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	5,7,12,17,18	2,6,9,11,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	5,7,12,16	2,6,9,11	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	5,7,12,17	2,6,9,11,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	5,7,12,16,18	2,6,9,11,15,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	5,7,12,14	2,6,9,11	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	5,7,12,14,16,17,18	2,6,9,11,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	5,7,12,14,18	2,6,9,11,15,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	5,7,12,14,16,17	2,6,9,11,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	5,7,12,17	2,6,9,11,13,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	5,7,12,16,18	2,6,9,11,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	5,7,12,17,18	2,6,9,11,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	5,7,12,16	2,6,9,11,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	5,7,12,14,18	2,6,9,11,13,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	5,7,12,14,16,17	2,6,9,11,13,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	5,7,12,14	2,6,9,11,13,15	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	5,7,12,14,16,17,18	2,6,9,11,13,15,17,18	2^{-12}

Table 0.631 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	5,7,10,17	2,6,9,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	5,7,10,16,18	2,6,9,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	5,7,10,17,18	2,6,9,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	5,7,10,16	2,6,9,15	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	5,7,10,14,18	2,6,9,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	5,7,10,14,16,17	2,6,9,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	5,7,10,14	2,6,9,15	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	5,7,10,14,16,17,18	2,6,9,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	5,7,10,17,18	2,6,9,13,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	5,7,10,16	2,6,9,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	5,7,10,17	2,6,9,13,15,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	5,7,10,16,18	2,6,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	5,7,10,14	2,6,9,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	5,7,10,14,16,17,18	2,6,9,13,17,18	2^{-34}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	5,7,10,14,18	2,6,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	5,7,10,14,16,17	2,6,9,13,15,17	2^{-34}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	5,7,10,12,18	2,6,9,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	5,7,10,12,16,17	2,6,9,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	5,7,10,12	2,6,9,15	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	5,7,10,12,16,17,18	2,6,9,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	5,7,10,12,14,17	2,6,9,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	5,7,10,12,14,16,18	2,6,9,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	5,7,10,12,14,17,18	2,6,9,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	5,7,10,12,14,16	2,6,9,15	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	5,7,10,12	2,6,9,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	5,7,10,12,16,17,18	2,6,9,13,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	5,7,10,12,18	2,6,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	5,7,10,12,16,17	2,6,9,13,15,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	5,7,10,12,14,17,18	2,6,9,13,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	5,7,10,12,14,16	2,6,9,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	5,7,10,12,14,17	2,6,9,13,15,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	5,7,10,12,14,16,18	2,6,9,13,15,18	$2^{-17.5}$

Table 0.632 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	5,7,10,17,18	2,6,9,11,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	5,7,10,16	2,6,9,11	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	5,7,10,17	2,6,9,11,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	5,7,10,16,18	2,6,9,11,15,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	5,7,10,14	2,6,9,11	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	5,7,10,14,16,17,18	2,6,9,11,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	5,7,10,14,18	2,6,9,11,15,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	5,7,10,14,16,17	2,6,9,11,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	5,7,10,17	2,6,9,11,13,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	5,7,10,16,18	2,6,9,11,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	5,7,10,17,18	2,6,9,11,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	5,7,10,16	2,6,9,11,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	5,7,10,14,18	2,6,9,11,13,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	5,7,10,14,16,17	2,6,9,11,13,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	5,7,10,14	2,6,9,11,13,15	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	5,7,10,14,16,17,18	2,6,9,11,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	5,7,10,12	2,6,9,11	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	5,7,10,12,16,17,18	2,6,9,11,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	5,7,10,12,18	2,6,9,11,15,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	5,7,10,12,16,17	2,6,9,11,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	5,7,10,12,14,17,18	2,6,9,11,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	5,7,10,12,14,16	2,6,9,11	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	5,7,10,12,14,17	2,6,9,11,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	5,7,10,12,14,16,18	2,6,9,11,15,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	5,7,10,12,18	2,6,9,11,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	5,7,10,12,16,17	2,6,9,11,13,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	5,7,10,12	2,6,9,11,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	5,7,10,12,16,17,18	2,6,9,11,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	5,7,10,12,14,17	2,6,9,11,13,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	5,7,10,12,14,16,18	2,6,9,11,13,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	5,7,10,12,14,17,18	2,6,9,11,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	5,7,10,12,14,16	2,6,9,11,13,15	$2^{-28.5}$

Table 0.633 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	5,7,17,18	2,6,8,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	5,7,16	2,6,8	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	5,7,17	2,6,8,15,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	5,7,16,18	2,6,8,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	5,7,14	2,6,8	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	5,7,14,16,17,18	2,6,8,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	5,7,14,18	2,6,8,15,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	5,7,14,16,17	2,6,8,15,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	5,7,17	2,6,8,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	5,7,16,18	2,6,8,13,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	5,7,17,18	2,6,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	5,7,16	2,6,8,13,15	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	5,7,14,18	2,6,8,13,18	2^{-34}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	5,7,14,16,17	2,6,8,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	5,7,14	2,6,8,13,15	2^{-34}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	5,7,14,16,17,18	2,6,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	5,7,12	2,6,8	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	5,7,12,16,17,18	2,6,8,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	5,7,12,18	2,6,8,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	5,7,12,16,17	2,6,8,15,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	5,7,12,14,17,18	2,6,8,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	5,7,12,14,16	2,6,8	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	5,7,12,14,17	2,6,8,15,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	5,7,12,14,16,18	2,6,8,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	5,7,12,18	2,6,8,13,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	5,7,12,16,17	2,6,8,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	5,7,12	2,6,8,13,15	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	5,7,12,16,17,18	2,6,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	5,7,12,14,17	2,6,8,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	5,7,12,14,16,18	2,6,8,13,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	5,7,12,14,17,18	2,6,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	5,7,12,14,16	2,6,8,13,15	2^{-12}

Table 0.634 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	5,7,17	2,6,8,11,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	5,7,16,18	2,6,8,11,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	5,7,17,18	2,6,8,11,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	5,7,16	2,6,8,11,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	5,7,14,18	2,6,8,11,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	5,7,14,16,17	2,6,8,11,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	5,7,14	2,6,8,11,15	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	5,7,14,16,17,18	2,6,8,11,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	5,7,17,18	2,6,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	5,7,16	2,6,8,11,13	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	5,7,17	2,6,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	5,7,16,18	2,6,8,11,13,15,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	5,7,14	2,6,8,11,13	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	5,7,14,16,17,18	2,6,8,11,13,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	5,7,14,18	2,6,8,11,13,15,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	5,7,14,16,17	2,6,8,11,13,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	5,7,12,18	2,6,8,11,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	5,7,12,16,17	2,6,8,11,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	5,7,12	2,6,8,11,15	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	5,7,12,16,17,18	2,6,8,11,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	5,7,12,14,17	2,6,8,11,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	5,7,12,14,16,18	2,6,8,11,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	5,7,12,14,17,18	2,6,8,11,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	5,7,12,14,16	2,6,8,11,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	5,7,12	2,6,8,11,13	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	5,7,12,16,17,18	2,6,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	5,7,12,18	2,6,8,11,13,15,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	5,7,12,16,17	2,6,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	5,7,12,14,17,18	2,6,8,11,13,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	5,7,12,14,16	2,6,8,11,13	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	5,7,12,14,17	2,6,8,11,13,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	5,7,12,14,16,18	2,6,8,11,13,15,18	2^{-23}

Table 0.635 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	5,7,10	2,6,8	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	5,7,10,16,17,18	2,6,8,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	5,7,10,18	2,6,8,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	5,7,10,16,17	2,6,8,15,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	5,7,10,14,17,18	2,6,8,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	5,7,10,14,16	2,6,8	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	5,7,10,14,17	2,6,8,15,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	5,7,10,14,16,18	2,6,8,15,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	5,7,10,18	2,6,8,13,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	5,7,10,16,17	2,6,8,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	5,7,10	2,6,8,13,15	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	5,7,10,16,17,18	2,6,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	5,7,10,14,17	2,6,8,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	5,7,10,14,16,18	2,6,8,13,18	2^{-1}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	5,7,10,14,17,18	2,6,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	5,7,10,14,16	2,6,8,13,15	2^{-1}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	5,7,10,12,17,18	2,6,8,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	5,7,10,12,16	2,6,8	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	5,7,10,12,17	2,6,8,15,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	5,7,10,12,16,18	2,6,8,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	5,7,10,12,14	2,6,8	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	5,7,10,12,14,16,17,18	2,6,8,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	5,7,10,12,14,18	2,6,8,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	5,7,10,12,14,16,17	2,6,8,15,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	5,7,10,12,17	2,6,8,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	5,7,10,12,16,18	2,6,8,13,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	5,7,10,12,17,18	2,6,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	5,7,10,12,16	2,6,8,13,15	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	5,7,10,12,14,18	2,6,8,13,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	5,7,10,12,14,16,17	2,6,8,13,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	5,7,10,12,14	2,6,8,13,15	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	5,7,10,12,14,16,17,18	2,6,8,13,15,17,18	$2^{-17.5}$

Table 0.636 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	5,7,10,18	2,6,8,11,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	5,7,10,16,17	2,6,8,11,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	5,7,10	2,6,8,11,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	5,7,10,16,17,18	2,6,8,11,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	5,7,10,14,17	2,6,8,11,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	5,7,10,14,16,18	2,6,8,11,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	5,7,10,14,17,18	2,6,8,11,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	5,7,10,14,16	2,6,8,11,15	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	5,7,10	2,6,8,11,13	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	5,7,10,16,17,18	2,6,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	5,7,10,18	2,6,8,11,13,15,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	5,7,10,16,17	2,6,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	5,7,10,14,17,18	2,6,8,11,13,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	5,7,10,14,16	2,6,8,11,13	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	5,7,10,14,17	2,6,8,11,13,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	5,7,10,14,16,18	2,6,8,11,13,15,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	5,7,10,12,17	2,6,8,11,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	5,7,10,12,16,18	2,6,8,11,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	5,7,10,12,17,18	2,6,8,11,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	5,7,10,12,16	2,6,8,11,15	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	5,7,10,12,14,18	2,6,8,11,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	5,7,10,12,14,16,17	2,6,8,11,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	5,7,10,12,14	2,6,8,11,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	5,7,10,12,14,16,17,18	2,6,8,11,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	5,7,10,12,17,18	2,6,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	5,7,10,12,16	2,6,8,11,13	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	5,7,10,12,17	2,6,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	5,7,10,12,16,18	2,6,8,11,13,15,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	5,7,10,12,14	2,6,8,11,13	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	5,7,10,12,14,16,17,18	2,6,8,11,13,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	5,7,10,12,14,18	2,6,8,11,13,15,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	5,7,10,12,14,16,17	2,6,8,11,13,15,17	$2^{-6.5}$

Table 0.637 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	5,7,17	2,6,8,9,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	5,7,16,18	2,6,8,9,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	5,7,17,18	2,6,8,9,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	5,7,16	2,6,8,9,15	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	5,7,14,18	2,6,8,9,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	5,7,14,16,17	2,6,8,9,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	5,7,14	2,6,8,9,15	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	5,7,14,16,17,18	2,6,8,9,15,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	5,7,17,18	2,6,8,9,13,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	5,7,16	2,6,8,9,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	5,7,17	2,6,8,9,13,15,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	5,7,16,18	2,6,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	5,7,14	2,6,8,9,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	5,7,14,16,17,18	2,6,8,9,13,17,18	2^{-1}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	5,7,14,18	2,6,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	5,7,14,16,17	2,6,8,9,13,15,17	2^{-1}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	5,7,12,18	2,6,8,9,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	5,7,12,16,17	2,6,8,9,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	5,7,12	2,6,8,9,15	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	5,7,12,16,17,18	2,6,8,9,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	5,7,12,14,17	2,6,8,9,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	5,7,12,14,16,18	2,6,8,9,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	5,7,12,14,17,18	2,6,8,9,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	5,7,12,14,16	2,6,8,9,15	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	5,7,12	2,6,8,9,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	5,7,12,16,17,18	2,6,8,9,13,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	5,7,12,18	2,6,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	5,7,12,16,17	2,6,8,9,13,15,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	5,7,12,14,17,18	2,6,8,9,13,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	5,7,12,14,16	2,6,8,9,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	5,7,12,14,17	2,6,8,9,13,15,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	5,7,12,14,16,18	2,6,8,9,13,15,18	$2^{-17.5}$

Table 0.638 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	5,7,17,18	2,6,8,9,11,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	5,7,16	2,6,8,9,11	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	5,7,17	2,6,8,9,11,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	5,7,16,18	2,6,8,9,11,15,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	5,7,14	2,6,8,9,11	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	5,7,14,16,17,18	2,6,8,9,11,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	5,7,14,18	2,6,8,9,11,15,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	5,7,14,16,17	2,6,8,9,11,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	5,7,17	2,6,8,9,11,13,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	5,7,16,18	2,6,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	5,7,17,18	2,6,8,9,11,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	5,7,16	2,6,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	5,7,14,18	2,6,8,9,11,13,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	5,7,14,16,17	2,6,8,9,11,13,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	5,7,14	2,6,8,9,11,13,15	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	5,7,14,16,17,18	2,6,8,9,11,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	5,7,12	2,6,8,9,11	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	5,7,12,16,17,18	2,6,8,9,11,17,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	5,7,12,18	2,6,8,9,11,15,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	5,7,12,16,17	2,6,8,9,11,15,17	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	5,7,12,14,17,18	2,6,8,9,11,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	5,7,12,14,16	2,6,8,9,11	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	5,7,12,14,17	2,6,8,9,11,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	5,7,12,14,16,18	2,6,8,9,11,15,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	5,7,12,18	2,6,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	5,7,12,16,17	2,6,8,9,11,13,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	5,7,12	2,6,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	5,7,12,16,17,18	2,6,8,9,11,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	5,7,12,14,17	2,6,8,9,11,13,17	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	5,7,12,14,16,18	2,6,8,9,11,13,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	5,7,12,14,17,18	2,6,8,9,11,13,15,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	5,7,12,14,16	2,6,8,9,11,13,15	$2^{-6.5}$

Table 0.639 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	5,7,10,18	2,6,8,9,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	5,7,10,16,17	2,6,8,9,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	5,7,10	2,6,8,9,15	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	5,7,10,16,17,18	2,6,8,9,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	5,7,10,14,17	2,6,8,9,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	5,7,10,14,16,18	2,6,8,9,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	5,7,10,14,17,18	2,6,8,9,15,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	5,7,10,14,16	2,6,8,9,15	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	5,7,10	2,6,8,9,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	5,7,10,16,17,18	2,6,8,9,13,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	5,7,10,18	2,6,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	5,7,10,16,17	2,6,8,9,13,15,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	5,7,10,14,17,18	2,6,8,9,13,17,18	2^{-34}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	5,7,10,14,16	2,6,8,9,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	5,7,10,14,17	2,6,8,9,13,15,17	2^{-34}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	5,7,10,14,16,18	2,6,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	5,7,10,12,17	2,6,8,9,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	5,7,10,12,16,18	2,6,8,9,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	5,7,10,12,17,18	2,6,8,9,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	5,7,10,12,16	2,6,8,9,15	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	5,7,10,12,14,18	2,6,8,9,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	5,7,10,12,14,16,17	2,6,8,9,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	5,7,10,12,14	2,6,8,9,15	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	5,7,10,12,14,16,17,18	2,6,8,9,15,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	5,7,10,12,17,18	2,6,8,9,13,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	5,7,10,12,16	2,6,8,9,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	5,7,10,12,17	2,6,8,9,13,15,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	5,7,10,12,16,18	2,6,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	5,7,10,12,14	2,6,8,9,13	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	5,7,10,12,14,16,17,18	2,6,8,9,13,17,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	5,7,10,12,14,18	2,6,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	5,7,10,12,14,16,17	2,6,8,9,13,15,17	2^{-12}

Table 0.640 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	5,7,10	2,6,8,9,11	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	5,7,10,16,17,18	2,6,8,9,11,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	5,7,10,18	2,6,8,9,11,15,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	5,7,10,16,17	2,6,8,9,11,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	5,7,10,14,17,18	2,6,8,9,11,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	5,7,10,14,16	2,6,8,9,11	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	5,7,10,14,17	2,6,8,9,11,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	5,7,10,14,16,18	2,6,8,9,11,15,18	2^{-12}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	5,7,10,18	2,6,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	5,7,10,16,17	2,6,8,9,11,13,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	5,7,10	2,6,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	5,7,10,16,17,18	2,6,8,9,11,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	5,7,10,14,17	2,6,8,9,11,13,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	5,7,10,14,16,18	2,6,8,9,11,13,18	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	5,7,10,14,17,18	2,6,8,9,11,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	5,7,10,14,16	2,6,8,9,11,13,15	$2^{-6.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	5,7,10,12,17,18	2,6,8,9,11,17,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	5,7,10,12,16	2,6,8,9,11	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	5,7,10,12,17	2,6,8,9,11,15,17	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	5,7,10,12,16,18	2,6,8,9,11,15,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	5,7,10,12,14	2,6,8,9,11	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	5,7,10,12,14,16,17,18	2,6,8,9,11,17,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	5,7,10,12,14,18	2,6,8,9,11,15,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	5,7,10,12,14,16,17	2,6,8,9,11,15,17	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	5,7,10,12,17	2,6,8,9,11,13,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	5,7,10,12,16,18	2,6,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	5,7,10,12,17,18	2,6,8,9,11,13,15,17,18	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	5,7,10,12,16	2,6,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	5,7,10,12,14,18	2,6,8,9,11,13,18	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	5,7,10,12,14,16,17	2,6,8,9,11,13,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	5,7,10,12,14,16,17	2,6,8,9,11,13,17	2^{-23}
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	5,7,10,12,14	2,6,8,9,11,13,15	$2^{-28.5}$
$(0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	5,7,10,12,14,16,17,18	2,6,8,9,11,13,15,17,18	2^{-23}

Table 0.641 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	—	2,4	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	16,17,18	2,4,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	18	2,4,15,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	16,17	2,4,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	14,17,18	2,4,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	14,16	2,4	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	14,17	2,4,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	14,16,18	2,4,15,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	18	2,4,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	16,17	2,4,13,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	—	2,4,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	16,17,18	2,4,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	14,17	2,4,13,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	14,16,18	2,4,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	14,17,18	2,4,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	14,16	2,4,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	12,17,18	2,4,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	12,16	2,4	2^{-34}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	12,17	2,4,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	12,16,18	2,4,15,18	2^{-34}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	12,14	2,4	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	12,14,16,17,18	2,4,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	12,14,18	2,4,15,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	12,14,16,17	2,4,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	12,17	2,4,13,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	12,16,18	2,4,13,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	12,17,18	2,4,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	12,16	2,4,13,15	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	12,14,18	2,4,13,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	12,14,16,17	2,4,13,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	12,14	2,4,13,15	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	12,14,16,17,18	2,4,13,15,17,18	2^{-23}

Table 0.642 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	18	2,4,11,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	16,17	2,4,11,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	—	2,4,11,15	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	16,17,18	2,4,11,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	14,17	2,4,11,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	14,16,18	2,4,11,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	14,17,18	2,4,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	14,16	2,4,11,15	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	—	2,4,11,13	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	16,17,18	2,4,11,13,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	18	2,4,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	16,17	2,4,11,13,15,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	14,17,18	2,4,11,13,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	14,16	2,4,11,13	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	14,17	2,4,11,13,15,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	14,16,18	2,4,11,13,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	12,17	2,4,11,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	12,16,18	2,4,11,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	12,17,18	2,4,11,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	12,16	2,4,11,15	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	12,14,18	2,4,11,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	12,14,16,17	2,4,11,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	12,14	2,4,11,15	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	12,14,16,17,18	2,4,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	12,17,18	2,4,11,13,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	12,16	2,4,11,13	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	12,17	2,4,11,13,15,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	12,16,18	2,4,11,13,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	12,14	2,4,11,13	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	12,14,16,17,18	2,4,11,13,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	12,14,18	2,4,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	12,14,16,17	2,4,11,13,15,17	2^{-12}

Table 0.643 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	10,17,18	2,4,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	10,16	2,4	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	10,17	2,4,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	10,16,18	2,4,15,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	10,14	2,4	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	10,14,16,17,18	2,4,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	10,14,18	2,4,15,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	10,14,16,17	2,4,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	10,17	2,4,13,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	10,16,18	2,4,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	10,17,18	2,4,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	10,16	2,4,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	10,14,18	2,4,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	10,14,16,17	2,4,13,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	10,14	2,4,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	10,14,16,17,18	2,4,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	10,12	2,4	2^{-1}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	10,12,16,17,18	2,4,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	10,12,18	2,4,15,18	2^{-1}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	10,12,16,17	2,4,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	10,12,14,17,18	2,4,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	10,12,14,16	2,4	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	10,12,14,17	2,4,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	10,12,14,16,18	2,4,15,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	10,12,18	2,4,13,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	10,12,16,17	2,4,13,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	10,12	2,4,13,15	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	10,12,16,17,18	2,4,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	10,12,14,17	2,4,13,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	10,12,14,16,18	2,4,13,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	10,12,14,17,18	2,4,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	10,12,14,16	2,4,13,15	$2^{-6.5}$

Table 0.644 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	10,17	2,4,11,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	10,16,18	2,4,11,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	10,17,18	2,4,11,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	10,16	2,4,11,15	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	10,14,18	2,4,11,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	10,14,16,17	2,4,11,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	10,14	2,4,11,15	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	10,14,16,17,18	2,4,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	10,17,18	2,4,11,13,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	10,16	2,4,11,13	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	10,17	2,4,11,13,15,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	10,16,18	2,4,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	10,14	2,4,11,13	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	10,14,16,17,18	2,4,11,13,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	10,14,18	2,4,11,13,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	10,14,16,17	2,4,11,13,15,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	10,12,18	2,4,11,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	10,12,16,17	2,4,11,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	10,12	2,4,11,15	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	10,12,16,17,18	2,4,11,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	10,12,14,17	2,4,11,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	10,12,14,16,18	2,4,11,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	10,12,14,17,18	2,4,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	10,12,14,16	2,4,11,15	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	10,12	2,4,11,13	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	10,12,16,17,18	2,4,11,13,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	10,12,18	2,4,11,13,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	10,12,16,17	2,4,11,13,15,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	10,12,14,17,18	2,4,11,13,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	10,12,14,16	2,4,11,13	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	10,12,14,17	2,4,11,13,15,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	10,12,14,16,18	2,4,11,13,15,18	$2^{-17.5}$

Table 0.645 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	18	2,4,9,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	16,17	2,4,9,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	—	2,4,9,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	16,17,18	2,4,9,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	14,17	2,4,9,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	14,16,18	2,4,9,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	14,17,18	2,4,9,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	14,16	2,4,9,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	—	2,4,9,13	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	16,17,18	2,4,9,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	18	2,4,9,13,15,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	16,17	2,4,9,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	14,17,18	2,4,9,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	14,16	2,4,9,13	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	14,17	2,4,9,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	14,16,18	2,4,9,13,15,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	12,17	2,4,9,17	2^{-1}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	12,16,18	2,4,9,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	12,17,18	2,4,9,15,17,18	2^{-1}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	12,16	2,4,9,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	12,14,18	2,4,9,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	12,14,16,17	2,4,9,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	12,14	2,4,9,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	12,14,16,17,18	2,4,9,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	12,17,18	2,4,9,13,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	12,16	2,4,9,13	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	12,17	2,4,9,13,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	12,16,18	2,4,9,13,15,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	12,14	2,4,9,13	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	12,14,16,17,18	2,4,9,13,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	12,14,18	2,4,9,13,15,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	12,14,16,17	2,4,9,13,15,17	$2^{-6.5}$

Table 0.646 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	—	2,4,9,11	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	16,17,18	2,4,9,11,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	18	2,4,9,11,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	16,17	2,4,9,11,15,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	14,17,18	2,4,9,11,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	14,16	2,4,9,11	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	14,17	2,4,9,11,15,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	14,16,18	2,4,9,11,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	18	2,4,9,11,13,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	16,17	2,4,9,11,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	—	2,4,9,11,13,15	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	16,17,18	2,4,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	14,17	2,4,9,11,13,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	14,16,18	2,4,9,11,13,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	14,17,18	2,4,9,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	14,16	2,4,9,11,13,15	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	12,17,18	2,4,9,11,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	12,16	2,4,9,11	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	12,17	2,4,9,11,15,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	12,16,18	2,4,9,11,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	12,14	2,4,9,11	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	12,14,16,17,18	2,4,9,11,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	12,14,18	2,4,9,11,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	12,14,16,17	2,4,9,11,15,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	12,17	2,4,9,11,13,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	12,16,18	2,4,9,11,13,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	12,17,18	2,4,9,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	12,16	2,4,9,11,13,15	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	12,14,18	2,4,9,11,13,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	12,14,16,17	2,4,9,11,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	12,14	2,4,9,11,13,15	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	12,14,16,17,18	2,4,9,11,13,15,17,18	$2^{-17.5}$

Table 0.647 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	10,17	2,4,9,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	10,16,18	2,4,9,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	10,17,18	2,4,9,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	10,16	2,4,9,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	10,14,18	2,4,9,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	10,14,16,17	2,4,9,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	10,14	2,4,9,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	10,14,16,17,18	2,4,9,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	10,17,18	2,4,9,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	10,16	2,4,9,13	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	10,17	2,4,9,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	10,16,18	2,4,9,13,15,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	10,14	2,4,9,13	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	10,14,16,17,18	2,4,9,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	10,14,18	2,4,9,13,15,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	10,14,16,17	2,4,9,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	10,12,18	2,4,9,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	10,12,16,17	2,4,9,17	2^{-34}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	10,12	2,4,9,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	10,12,16,17,18	2,4,9,15,17,18	2^{-34}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	10,12,14,17	2,4,9,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	10,12,14,16,18	2,4,9,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	10,12,14,17,18	2,4,9,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	10,12,14,16	2,4,9,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	10,12	2,4,9,13	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	10,12,16,17,18	2,4,9,13,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	10,12,18	2,4,9,13,15,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	10,12,16,17	2,4,9,13,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	10,12,14,17,18	2,4,9,13,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	10,12,14,16	2,4,9,13	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	10,12,14,17	2,4,9,13,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	10,12,14,16,18	2,4,9,13,15,18	2^{-23}

Table 0.648 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	10,17,18	2,4,9,11,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	10,16	2,4,9,11	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	10,17	2,4,9,11,15,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	10,16,18	2,4,9,11,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	10,14	2,4,9,11	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	10,14,16,17,18	2,4,9,11,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	10,14,18	2,4,9,11,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	10,14,16,17	2,4,9,11,15,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	10,17	2,4,9,11,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	10,16,18	2,4,9,11,13,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	10,17,18	2,4,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	10,16	2,4,9,11,13,15	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	10,14,18	2,4,9,11,13,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	10,14,16,17	2,4,9,11,13,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	10,14	2,4,9,11,13,15	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	10,14,16,17,18	2,4,9,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	10,12	2,4,9,11	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	10,12,16,17,18	2,4,9,11,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	10,12,18	2,4,9,11,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	10,12,16,17	2,4,9,11,15,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	10,12,14,17,18	2,4,9,11,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	10,12,14,16	2,4,9,11	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	10,12,14,17	2,4,9,11,15,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	10,12,14,16,18	2,4,9,11,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	10,12,18	2,4,9,11,13,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	10,12,16,17	2,4,9,11,13,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	10,12	2,4,9,11,13,15	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	10,12,16,17,18	2,4,9,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	10,12,14,17	2,4,9,11,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	10,12,14,16,18	2,4,9,11,13,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	10,12,14,17,18	2,4,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	10,12,14,16	2,4,9,11,13,15	2^{-12}

Table 0.649 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	17,18	2,4,8,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	16	2,4,8	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	17	2,4,8,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	16,18	2,4,8,15,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	14	2,4,8	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	14,16,17,18	2,4,8,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	14,18	2,4,8,15,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	14,16,17	2,4,8,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	17	2,4,8,13,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	16,18	2,4,8,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	17,18	2,4,8,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	16	2,4,8,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	14,18	2,4,8,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	14,16,17	2,4,8,13,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	14	2,4,8,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	14,16,17,18	2,4,8,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	12	2,4,8	2^{-34}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	12,16,17,18	2,4,8,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	12,18	2,4,8,15,18	2^{-34}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	12,16,17	2,4,8,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	12,14,17,18	2,4,8,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	12,14,16	2,4,8	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	12,14,17	2,4,8,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	12,14,16,18	2,4,8,15,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	12,18	2,4,8,13,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	12,16,17	2,4,8,13,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	12	2,4,8,13,15	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	12,16,17,18	2,4,8,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	12,14,17	2,4,8,13,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	12,14,16,18	2,4,8,13,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	12,14,17,18	2,4,8,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	12,14,16	2,4,8,13,15	$2^{-28.5}$

Table 0.650 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	17	2,4,8,11,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	16,18	2,4,8,11,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	17,18	2,4,8,11,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	16	2,4,8,11,15	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	14,18	2,4,8,11,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	14,16,17	2,4,8,11,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	14	2,4,8,11,15	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	14,16,17,18	2,4,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	17,18	2,4,8,11,13,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	16	2,4,8,11,13	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	17	2,4,8,11,13,15,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	16,18	2,4,8,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	14	2,4,8,11,13	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	14,16,17,18	2,4,8,11,13,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	14,18	2,4,8,11,13,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	14,16,17	2,4,8,11,13,15,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	12,18	2,4,8,11,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	12,16,17	2,4,8,11,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	12	2,4,8,11,15	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	12,16,17,18	2,4,8,11,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	12,14,17	2,4,8,11,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	12,14,16,18	2,4,8,11,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	12,14,17,18	2,4,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	12,14,16	2,4,8,11,15	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	12	2,4,8,11,13	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	12,16,17,18	2,4,8,11,13,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	12,18	2,4,8,11,13,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	12,16,17	2,4,8,11,13,15,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	12,14,17,18	2,4,8,11,13,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	12,14,16	2,4,8,11,13	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	12,14,17	2,4,8,11,13,15,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	12,14,16,18	2,4,8,11,13,15,18	$2^{-17.5}$

Table 0.651 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	10	2,4,8	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	10,16,17,18	2,4,8,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	10,18	2,4,8,15,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	10,16,17	2,4,8,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	10,14,17,18	2,4,8,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	10,14,16	2,4,8	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	10,14,17	2,4,8,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	10,14,16,18	2,4,8,15,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	10,18	2,4,8,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	10,16,17	2,4,8,13,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	10	2,4,8,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	10,16,17,18	2,4,8,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	10,14,17	2,4,8,13,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	10,14,16,18	2,4,8,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	10,14,17,18	2,4,8,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	10,14,16	2,4,8,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	10,12,17,18	2,4,8,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	10,12,16	2,4,8	2^{-1}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	10,12,17	2,4,8,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	10,12,16,18	2,4,8,15,18	2^{-1}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	10,12,14	2,4,8	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	10,12,14,16,17,18	2,4,8,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	10,12,14,18	2,4,8,15,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	10,12,14,16,17	2,4,8,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	10,12,17	2,4,8,13,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	10,12,16,18	2,4,8,13,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	10,12,17,18	2,4,8,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	10,12,16	2,4,8,13,15	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	10,12,14,18	2,4,8,13,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	10,12,14,16,17	2,4,8,13,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	10,12,14	2,4,8,13,15	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	10,12,14,16,17,18	2,4,8,13,15,17,18	2^{-12}

Table 0.652 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	10,18	2,4,8,11,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	10,16,17	2,4,8,11,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	10	2,4,8,11,15	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	10,16,17,18	2,4,8,11,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	10,14,17	2,4,8,11,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	10,14,16,18	2,4,8,11,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	10,14,17,18	2,4,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	10,14,16	2,4,8,11,15	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	10	2,4,8,11,13	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	10,16,17,18	2,4,8,11,13,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	10,18	2,4,8,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	10,16,17	2,4,8,11,13,15,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	10,14,17,18	2,4,8,11,13,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	10,14,16	2,4,8,11,13	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	10,14,17	2,4,8,11,13,15,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	10,14,16,18	2,4,8,11,13,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	10,12,17	2,4,8,11,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	10,12,16,18	2,4,8,11,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	10,12,17,18	2,4,8,11,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	10,12,16	2,4,8,11,15	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	10,12,14,18	2,4,8,11,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	10,12,14,16,17	2,4,8,11,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	10,12,14	2,4,8,11,15	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	10,12,14,16,17,18	2,4,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	10,12,17,18	2,4,8,11,13,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	10,12,16	2,4,8,11,13	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	10,12,17	2,4,8,11,13,15,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	10,12,16,18	2,4,8,11,13,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	10,12,14	2,4,8,11,13	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	10,12,14,16,17,18	2,4,8,11,13,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	10,12,14,18	2,4,8,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	10,12,14,16,17	2,4,8,11,13,15,17	2^{-23}

Table 0.653 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	17	2,4,8,9,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	16,18	2,4,8,9,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	17,18	2,4,8,9,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	16	2,4,8,9,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	14,18	2,4,8,9,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	14,16,17	2,4,8,9,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	14	2,4,8,9,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	14,16,17,18	2,4,8,9,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	17,18	2,4,8,9,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	16	2,4,8,9,13	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	17	2,4,8,9,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	16,18	2,4,8,9,13,15,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	14	2,4,8,9,13	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	14,16,17,18	2,4,8,9,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	14,18	2,4,8,9,13,15,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	14,16,17	2,4,8,9,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	12,18	2,4,8,9,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	12,16,17	2,4,8,9,17	2^{-1}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	12	2,4,8,9,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	12,16,17,18	2,4,8,9,15,17,18	2^{-1}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	12,14,17	2,4,8,9,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	12,14,16,18	2,4,8,9,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	12,14,17,18	2,4,8,9,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	12,14,16	2,4,8,9,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	12	2,4,8,9,13	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	12,16,17,18	2,4,8,9,13,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	12,18	2,4,8,9,13,15,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	12,16,17	2,4,8,9,13,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	12,14,17,18	2,4,8,9,13,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	12,14,16	2,4,8,9,13	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	12,14,17	2,4,8,9,13,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	12,14,16,18	2,4,8,9,13,15,18	2^{-12}

Table 0.654 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	17,18	2,4,8,9,11,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	16	2,4,8,9,11	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	17	2,4,8,9,11,15,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	16,18	2,4,8,9,11,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	14	2,4,8,9,11	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	14,16,17,18	2,4,8,9,11,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	14,18	2,4,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	14,16,17	2,4,8,9,11,15,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	17	2,4,8,9,11,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	16,18	2,4,8,9,11,13,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	17,18	2,4,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	16	2,4,8,9,11,13,15	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	14,18	2,4,8,9,11,13,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	14,16,17	2,4,8,9,11,13,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	14	2,4,8,9,11,13,15	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	14,16,17,18	2,4,8,9,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	12	2,4,8,9,11	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	12,16,17,18	2,4,8,9,11,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	12,18	2,4,8,9,11,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	12,16,17	2,4,8,9,11,15,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	12,14,17,18	2,4,8,9,11,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	12,14,16	2,4,8,9,11	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	12,14,17	2,4,8,9,11,15,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	12,14,16,18	2,4,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	12,18	2,4,8,9,11,13,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	12,16,17	2,4,8,9,11,13,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	12	2,4,8,9,11,13,15	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	12,16,17,18	2,4,8,9,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	12,14,17	2,4,8,9,11,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	12,14,16,18	2,4,8,9,11,13,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	12,14,17,18	2,4,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	12,14,16	2,4,8,9,11,13,15	2^{-23}

Table 0.655 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	10,18	2,4,8,9,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	10,16,17	2,4,8,9,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	10	2,4,8,9,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	10,16,17,18	2,4,8,9,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	10,14,17	2,4,8,9,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	10,14,16,18	2,4,8,9,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	10,14,17,18	2,4,8,9,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	10,14,16	2,4,8,9,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	10	2,4,8,9,13	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	10,16,17,18	2,4,8,9,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	10,18	2,4,8,9,13,15,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	10,16,17	2,4,8,9,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	10,14,17,18	2,4,8,9,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	10,14,16	2,4,8,9,13	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	10,14,17	2,4,8,9,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	10,14,16,18	2,4,8,9,13,15,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	10,12,17	2,4,8,9,17	2^{-34}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	10,12,16,18	2,4,8,9,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	10,12,17,18	2,4,8,9,15,17,18	2^{-34}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	10,12,16	2,4,8,9,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	10,12,14,18	2,4,8,9,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	10,12,14,16,17	2,4,8,9,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	10,12,14	2,4,8,9,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	10,12,14,16,17,18	2,4,8,9,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	10,12,17,18	2,4,8,9,13,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	10,12,16	2,4,8,9,13	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	10,12,17	2,4,8,9,13,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	10,12,16,18	2,4,8,9,13,15,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	10,12,14	2,4,8,9,13	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	10,12,14,16,17,18	2,4,8,9,13,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	10,12,14,18	2,4,8,9,13,15,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	10,12,14,16,17	2,4,8,9,13,15,17	$2^{-28.5}$

Table 0.656 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	10	2,4,8,9,11	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	10,16,17,18	2,4,8,9,11,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	10,18	2,4,8,9,11,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	10,16,17	2,4,8,9,11,15,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	10,14,17,18	2,4,8,9,11,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	10,14,16	2,4,8,9,11	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	10,14,17	2,4,8,9,11,15,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	10,14,16,18	2,4,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	10,18	2,4,8,9,11,13,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	10,16,17	2,4,8,9,11,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	10	2,4,8,9,11,13,15	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	10,16,17,18	2,4,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	10,14,17	2,4,8,9,11,13,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	10,14,16,18	2,4,8,9,11,13,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	10,14,17,18	2,4,8,9,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	10,14,16	2,4,8,9,11,13,15	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	10,12,17,18	2,4,8,9,11,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	10,12,16	2,4,8,9,11	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	10,12,17	2,4,8,9,11,15,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	10,12,16,18	2,4,8,9,11,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	10,12,14	2,4,8,9,11	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	10,12,14,16,17,18	2,4,8,9,11,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	10,12,14,18	2,4,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	10,12,14,16,17	2,4,8,9,11,15,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	10,12,17	2,4,8,9,11,13,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	10,12,16,18	2,4,8,9,11,13,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	10,12,17,18	2,4,8,9,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	10,12,16	2,4,8,9,11,13,15	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	10,12,14,18	2,4,8,9,11,13,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	10,12,14,16,17	2,4,8,9,11,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	10,12,14	2,4,8,9,11,13,15	2^{-12}
$(0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	10,12,14,16,17,18	2,4,8,9,11,13,15,17,18	$2^{-17.5}$

Table 0.657 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	7,18	2,4,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	7,16,17	2,4,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	7	2,4,15	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	7,16,17,18	2,4,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	7,14,17	2,4,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	7,14,16,18	2,4,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	7,14,17,18	2,4,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	7,14,16	2,4,15	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	7	2,4,13	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	7,16,17,18	2,4,13,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	7,18	2,4,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	7,16,17	2,4,13,15,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	7,14,17,18	2,4,13,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	7,14,16	2,4,13	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	7,14,17	2,4,13,15,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	7,14,16,18	2,4,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	7,12,17	2,4,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	7,12,16,18	2,4,18	2^{-34}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	7,12,17,18	2,4,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	7,12,16	2,4,15	2^{-34}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	7,12,14,18	2,4,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	7,12,14,16,17	2,4,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	7,12,14	2,4,15	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	7,12,14,16,17,18	2,4,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	7,12,17,18	2,4,13,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	7,12,16	2,4,13	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	7,12,17	2,4,13,15,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	7,12,16,18	2,4,13,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	7,12,14	2,4,13	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	7,12,14,16,17,18	2,4,13,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	7,12,14,18	2,4,13,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	7,12,14,16,17	2,4,13,15,17	2^{-23}

Table 0.658 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	7	2,4,11	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	7,16,17,18	2,4,11,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	7,18	2,4,11,15,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	7,16,17	2,4,11,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	7,14,17,18	2,4,11,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	7,14,16	2,4,11	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	7,14,17	2,4,11,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	7,14,16,18	2,4,11,15,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	7,18	2,4,11,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	7,16,17	2,4,11,13,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	7	2,4,11,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	7,16,17,18	2,4,11,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	7,14,17	2,4,11,13,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	7,14,16,18	2,4,11,13,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	7,14,17,18	2,4,11,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	7,14,16	2,4,11,13,15	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	7,12,17,18	2,4,11,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	7,12,16	2,4,11	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	7,12,17	2,4,11,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	7,12,16,18	2,4,11,15,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	7,12,14	2,4,11	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	7,12,14,16,17,18	2,4,11,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	7,12,14,18	2,4,11,15,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	7,12,14,16,17	2,4,11,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	7,12,17	2,4,11,13,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	7,12,16,18	2,4,11,13,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	7,12,17,18	2,4,11,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	7,12,16	2,4,11,13,15	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	7,12,14,18	2,4,11,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	7,12,14,16,17	2,4,11,13,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	7,12,14	2,4,11,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	7,12,14,16,17,18	2,4,11,13,15,17,18	2^{-12}

Table 0.659 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(2)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	7,10,17	2,4,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	7,10,16,18	2,4,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	7,10,17,18	2,4,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	7,10,16	2,4,15	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	7,10,14,18	2,4,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	7,10,14,16,17	2,4,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	7,10,14	2,4,15	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	7,10,14,16,17,18	2,4,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	7,10,17,18	2,4,13,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	7,10,16	2,4,13	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	7,10,17	2,4,13,15,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	7,10,16,18	2,4,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	7,10,14	2,4,13	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	7,10,14,16,17,18	2,4,13,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	7,10,14,18	2,4,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	7,10,14,16,17	2,4,13,15,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	7,10,12,18	2,4,18	2^{-1}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	7,10,12,16,17	2,4,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	7,10,12	2,4,15	2^{-1}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	7,10,12,16,17,18	2,4,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	7,10,12,14,17	2,4,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	7,10,12,14,16,18	2,4,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	7,10,12,14,17,18	2,4,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	7,10,12,14,16	2,4,15	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	7,10,12	2,4,13	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	7,10,12,16,17,18	2,4,13,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	7,10,12,18	2,4,13,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	7,10,12,16,17	2,4,13,15,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	7,10,12,14,17,18	2,4,13,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	7,10,12,14,16	2,4,13	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	7,10,12,14,17	2,4,13,15,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	7,10,12,14,16,18	2,4,13,15,18	$2^{-6.5}$

Table 0.660 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	7,10,17,18	2,4,11,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	7,10,16	2,4,11	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	7,10,17	2,4,11,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	7,10,16,18	2,4,11,15,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	7,10,14	2,4,11	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	7,10,14,16,17,18	2,4,11,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	7,10,14,18	2,4,11,15,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	7,10,14,16,17	2,4,11,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	7,10,17	2,4,11,13,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	7,10,16,18	2,4,11,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	7,10,17,18	2,4,11,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	7,10,16	2,4,11,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	7,10,14,18	2,4,11,13,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	7,10,14,16,17	2,4,11,13,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	7,10,14	2,4,11,13,15	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	7,10,14,16,17,18	2,4,11,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	7,10,12	2,4,11	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	7,10,12,16,17,18	2,4,11,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	7,10,12,18	2,4,11,15,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	7,10,12,16,17	2,4,11,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	7,10,12,14,17,18	2,4,11,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	7,10,12,14,16	2,4,11	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	7,10,12,14,17	2,4,11,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	7,10,12,14,16,18	2,4,11,15,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	7,10,12,18	2,4,11,13,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	7,10,12,16,17	2,4,11,13,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	7,10,12	2,4,11,13,15	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	7,10,12,16,17,18	2,4,11,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	7,10,12,14,17	2,4,11,13,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	7,10,12,14,16,18	2,4,11,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	7,10,12,14,17,18	2,4,11,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	7,10,12,14,16	2,4,11,13,15	$2^{-17.5}$

Table 0.661 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	7	2,4,9	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	7,16,17,18	2,4,9,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	7,18	2,4,9,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	7,16,17	2,4,9,15,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	7,14,17,18	2,4,9,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	7,14,16	2,4,9	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	7,14,17	2,4,9,15,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	7,14,16,18	2,4,9,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	7,18	2,4,9,13,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	7,16,17	2,4,9,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	7	2,4,9,13,15	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	7,16,17,18	2,4,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	7,14,17	2,4,9,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	7,14,16,18	2,4,9,13,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	7,14,17,18	2,4,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	7,14,16	2,4,9,13,15	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	7,12,17,18	2,4,9,17,18	2^{-1}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	7,12,16	2,4,9	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	7,12,17	2,4,9,15,17	2^{-1}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	7,12,16,18	2,4,9,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	7,12,14	2,4,9	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	7,12,14,16,17,18	2,4,9,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	7,12,14,18	2,4,9,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	7,12,14,16,17	2,4,9,15,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	7,12,17	2,4,9,13,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	7,12,16,18	2,4,9,13,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	7,12,17,18	2,4,9,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	7,12,16	2,4,9,13,15	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	7,12,14,18	2,4,9,13,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	7,12,14,16,17	2,4,9,13,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	7,12,14	2,4,9,13,15	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	7,12,14,16,17,18	2,4,9,13,15,17,18	$2^{-6.5}$

Table 0.662 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	7,18	2,4,9,11,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	7,16,17	2,4,9,11,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	7	2,4,9,11,15	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	7,16,17,18	2,4,9,11,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	7,14,17	2,4,9,11,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	7,14,16,18	2,4,9,11,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	7,14,17,18	2,4,9,11,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	7,14,16	2,4,9,11,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	7	2,4,9,11,13	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	7,16,17,18	2,4,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	7,18	2,4,9,11,13,15,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	7,16,17	2,4,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	7,14,17,18	2,4,9,11,13,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	7,14,16	2,4,9,11,13	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	7,14,17	2,4,9,11,13,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	7,14,16,18	2,4,9,11,13,15,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	7,12,17	2,4,9,11,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	7,12,16,18	2,4,9,11,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	7,12,17,18	2,4,9,11,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	7,12,16	2,4,9,11,15	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	7,12,14,18	2,4,9,11,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	7,12,14,16,17	2,4,9,11,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	7,12,14	2,4,9,11,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	7,12,14,16,17,18	2,4,9,11,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	7,12,17,18	2,4,9,11,13,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	7,12,16	2,4,9,11,13	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	7,12,17	2,4,9,11,13,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	7,12,16,18	2,4,9,11,13,15,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	7,12,14	2,4,9,11,13	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	7,12,14,16,17,18	2,4,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	7,12,14,18	2,4,9,11,13,15,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	7,12,14,16,17	2,4,9,11,13,15,17	$2^{-17.5}$

Table 0.663 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	7,10,17,18	2,4,9,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	7,10,16	2,4,9	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	7,10,17	2,4,9,15,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	7,10,16,18	2,4,9,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	7,10,14	2,4,9	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	7,10,14,16,17,18	2,4,9,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	7,10,14,18	2,4,9,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	7,10,14,16,17	2,4,9,15,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	7,10,17	2,4,9,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	7,10,16,18	2,4,9,13,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	7,10,17,18	2,4,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	7,10,16	2,4,9,13,15	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	7,10,14,18	2,4,9,13,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	7,10,14,16,17	2,4,9,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	7,10,14	2,4,9,13,15	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	7,10,14,16,17,18	2,4,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	7,10,12	2,4,9	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	7,10,12,16,17,18	2,4,9,17,18	2^{-34}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	7,10,12,18	2,4,9,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	7,10,12,16,17	2,4,9,15,17	2^{-34}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	7,10,12,14,17,18	2,4,9,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	7,10,12,14,16	2,4,9	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	7,10,12,14,17	2,4,9,15,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	7,10,12,14,16,18	2,4,9,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	7,10,12,18	2,4,9,13,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	7,10,12,16,17	2,4,9,13,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	7,10,12	2,4,9,13,15	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	7,10,12,16,17,18	2,4,9,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	7,10,12,14,17	2,4,9,13,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	7,10,12,14,16,18	2,4,9,13,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	7,10,12,14,17,18	2,4,9,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	7,10,12,14,16	2,4,9,13,15	2^{-23}

Table 0.664 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	7,10,17	2,4,9,11,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	7,10,16,18	2,4,9,11,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	7,10,17,18	2,4,9,11,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	7,10,16	2,4,9,11,15	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	7,10,14,18	2,4,9,11,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	7,10,14,16,17	2,4,9,11,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	7,10,14	2,4,9,11,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	7,10,14,16,17,18	2,4,9,11,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	7,10,17,18	2,4,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	7,10,16	2,4,9,11,13	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	7,10,17	2,4,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	7,10,16,18	2,4,9,11,13,15,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	7,10,14	2,4,9,11,13	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	7,10,14,16,17,18	2,4,9,11,13,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	7,10,14,18	2,4,9,11,13,15,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	7,10,14,16,17	2,4,9,11,13,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	7,10,12,18	2,4,9,11,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	7,10,12,16,17	2,4,9,11,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	7,10,12	2,4,9,11,15	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	7,10,12,16,17,18	2,4,9,11,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	7,10,12,14,17	2,4,9,11,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	7,10,12,14,16,18	2,4,9,11,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	7,10,12,14,17,18	2,4,9,11,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	7,10,12,14,16	2,4,9,11,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	7,10,12	2,4,9,11,13	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	7,10,12,16,17,18	2,4,9,11,13,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	7,10,12,18	2,4,9,11,13,15,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	7,10,12,16,17	2,4,9,11,13,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	7,10,12,14,17,18	2,4,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	7,10,12,14,16	2,4,9,11,13	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	7,10,12,14,17	2,4,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	7,10,12,14,16,18	2,4,9,11,13,15,18	2^{-12}

Table 0.665 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	7,17	2,4,8,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	7,16,18	2,4,8,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	7,17,18	2,4,8,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	7,16	2,4,8,15	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	7,14,18	2,4,8,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	7,14,16,17	2,4,8,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	7,14	2,4,8,15	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	7,14,16,17,18	2,4,8,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	7,17,18	2,4,8,13,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	7,16	2,4,8,13	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	7,17	2,4,8,13,15,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	7,16,18	2,4,8,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	7,14	2,4,8,13	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	7,14,16,17,18	2,4,8,13,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	7,14,18	2,4,8,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	7,14,16,17	2,4,8,13,15,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	7,12,18	2,4,8,18	2^{-34}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	7,12,16,17	2,4,8,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	7,12	2,4,8,15	2^{-34}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	7,12,16,17,18	2,4,8,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	7,12,14,17	2,4,8,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	7,12,14,16,18	2,4,8,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	7,12,14,17,18	2,4,8,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	7,12,14,16	2,4,8,15	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	7,12	2,4,8,13	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	7,12,16,17,18	2,4,8,13,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	7,12,18	2,4,8,13,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	7,12,16,17	2,4,8,13,15,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	7,12,14,17,18	2,4,8,13,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	7,12,14,16	2,4,8,13	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	7,12,14,17	2,4,8,13,15,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	7,12,14,16,18	2,4,8,13,15,18	$2^{-28.5}$

Table 0.666 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	7,17,18	2,4,8,11,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	7,16	2,4,8,11	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	7,17	2,4,8,11,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	7,16,18	2,4,8,11,15,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	7,14	2,4,8,11	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	7,14,16,17,18	2,4,8,11,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	7,14,18	2,4,8,11,15,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	7,14,16,17	2,4,8,11,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	7,17	2,4,8,11,13,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	7,16,18	2,4,8,11,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	7,17,18	2,4,8,11,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	7,16	2,4,8,11,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	7,14,18	2,4,8,11,13,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	7,14,16,17	2,4,8,11,13,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	7,14	2,4,8,11,13,15	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	7,14,16,17,18	2,4,8,11,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	7,12	2,4,8,11	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	7,12,16,17,18	2,4,8,11,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	7,12,18	2,4,8,11,15,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	7,12,16,17	2,4,8,11,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	7,12,14,17,18	2,4,8,11,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	7,12,14,16	2,4,8,11	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	7,12,14,17	2,4,8,11,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	7,12,14,16,18	2,4,8,11,15,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	7,12,18	2,4,8,11,13,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	7,12,16,17	2,4,8,11,13,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	7,12	2,4,8,11,13,15	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	7,12,16,17,18	2,4,8,11,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	7,12,14,17	2,4,8,11,13,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	7,12,14,16,18	2,4,8,11,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	7,12,14,17,18	2,4,8,11,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	7,12,14,16	2,4,8,11,13,15	$2^{-17.5}$

Table 0.667 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	7,10,18	2,4,8,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	7,10,16,17	2,4,8,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	7,10	2,4,8,15	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	7,10,16,17,18	2,4,8,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	7,10,14,17	2,4,8,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	7,10,14,16,18	2,4,8,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	7,10,14,17,18	2,4,8,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	7,10,14,16	2,4,8,15	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	7,10	2,4,8,13	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	7,10,16,17,18	2,4,8,13,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	7,10,18	2,4,8,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	7,10,16,17	2,4,8,13,15,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	7,10,14,17,18	2,4,8,13,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	7,10,14,16	2,4,8,13	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	7,10,14,17	2,4,8,13,15,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	7,10,14,16,18	2,4,8,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	7,10,12,17	2,4,8,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	7,10,12,16,18	2,4,8,18	2^{-1}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	7,10,12,17,18	2,4,8,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	7,10,12,16	2,4,8,15	2^{-1}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	7,10,12,14,18	2,4,8,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	7,10,12,14,16,17	2,4,8,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	7,10,12,14	2,4,8,15	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	7,10,12,14,16,17,18	2,4,8,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	7,10,12,17,18	2,4,8,13,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	7,10,12,16	2,4,8,13	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	7,10,12,17	2,4,8,13,15,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	7,10,12,16,18	2,4,8,13,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	7,10,12,14	2,4,8,13	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	7,10,12,14,16,17,18	2,4,8,13,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	7,10,12,14,18	2,4,8,13,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	7,10,12,14,16,17	2,4,8,13,15,17	2^{-12}

Table 0.668 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	7,10	2,4,8,11	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	7,10,16,17,18	2,4,8,11,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	7,10,18	2,4,8,11,15,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	7,10,16,17	2,4,8,11,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	7,10,14,17,18	2,4,8,11,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	7,10,14,16	2,4,8,11	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	7,10,14,17	2,4,8,11,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	7,10,14,16,18	2,4,8,11,15,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	7,10,18	2,4,8,11,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	7,10,16,17	2,4,8,11,13,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	7,10	2,4,8,11,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	7,10,16,17,18	2,4,8,11,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	7,10,14,17	2,4,8,11,13,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	7,10,14,16,18	2,4,8,11,13,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	7,10,14,17,18	2,4,8,11,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	7,10,14,16	2,4,8,11,13,15	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	7,10,12,17,18	2,4,8,11,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	7,10,12,16	2,4,8,11	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	7,10,12,17	2,4,8,11,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	7,10,12,16,18	2,4,8,11,15,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	7,10,12,14	2,4,8,11	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	7,10,12,14,16,17,18	2,4,8,11,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	7,10,12,14,18	2,4,8,11,15,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	7,10,12,14,16,17	2,4,8,11,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	7,10,12,17	2,4,8,11,13,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	7,10,12,16,18	2,4,8,11,13,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	7,10,12,17,18	2,4,8,11,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	7,10,12,16	2,4,8,11,13,15	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	7,10,12,14,18	2,4,8,11,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	7,10,12,14,16,17	2,4,8,11,13,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	7,10,12,14	2,4,8,11,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	7,10,12,14,16,17,18	2,4,8,11,13,15,17,18	2^{-23}

Table 0.669 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	7,17,18	2,4,8,9,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	7,16	2,4,8,9	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	7,17	2,4,8,9,15,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	7,16,18	2,4,8,9,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	7,14	2,4,8,9	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	7,14,16,17,18	2,4,8,9,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	7,14,18	2,4,8,9,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	7,14,16,17	2,4,8,9,15,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	7,17	2,4,8,9,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	7,16,18	2,4,8,9,13,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	7,17,18	2,4,8,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	7,16	2,4,8,9,13,15	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	7,14,18	2,4,8,9,13,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	7,14,16,17	2,4,8,9,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	7,14	2,4,8,9,13,15	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	7,14,16,17,18	2,4,8,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	7,12	2,4,8,9	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	7,12,16,17,18	2,4,8,9,17,18	2^{-1}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	7,12,18	2,4,8,9,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	7,12,16,17	2,4,8,9,13,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	7,12	2,4,8,9,13,15	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	7,12,16,17,18	2,4,8,9,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	7,12,14,17	2,4,8,9,13,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	7,12,14,16,18	2,4,8,9,13,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	7,12,14,17,18	2,4,8,9,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	7,12,14,16	2,4,8,9,13,15	2^{-12}

Table 0.670 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	7,17	2,4,8,9,11,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	7,16,18	2,4,8,9,11,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	7,17,18	2,4,8,9,11,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	7,16	2,4,8,9,11,15	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	7,14,18	2,4,8,9,11,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	7,14,16,17	2,4,8,9,11,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	7,14	2,4,8,9,11,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	7,14,16,17,18	2,4,8,9,11,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	7,17,18	2,4,8,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	7,16	2,4,8,9,11,13	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	7,17	2,4,8,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	7,16,18	2,4,8,9,11,13,15,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	7,14	2,4,8,9,11,13	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	7,14,16,17,18	2,4,8,9,11,13,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	7,14,18	2,4,8,9,11,13,15,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	7,14,16,17	2,4,8,9,11,13,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	7,12,18	2,4,8,9,11,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	7,12,16,17	2,4,8,9,11,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	7,12	2,4,8,9,11,15	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	7,12,16,17,18	2,4,8,9,11,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	7,12,14,17	2,4,8,9,11,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	7,12,14,16,18	2,4,8,9,11,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	7,12,14,17,18	2,4,8,9,11,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	7,12,14,16	2,4,8,9,11,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	7,12	2,4,8,9,11,13	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	7,12,16,17,18	2,4,8,9,11,13,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	7,12,18	2,4,8,9,11,13,15,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	7,12,16,17	2,4,8,9,11,13,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	7,12,14,17,18	2,4,8,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	7,12,14,16	2,4,8,9,11,13	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	7,12,14,17	2,4,8,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	7,12,14,16,18	2,4,8,9,11,13,15,18	2^{-23}

Table 0.671 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	7,10	2,4,8,9	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	7,10,16,17,18	2,4,8,9,17,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	7,10,18	2,4,8,9,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	7,10,16,17	2,4,8,9,15,17	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	7,10,14,17,18	2,4,8,9,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	7,10,14,16	2,4,8,9	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	7,10,14,17	2,4,8,9,15,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	7,10,14,16,18	2,4,8,9,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	7,10,18	2,4,8,9,13,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	7,10,16,17	2,4,8,9,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	7,10	2,4,8,9,13,15	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	7,10,16,17,18	2,4,8,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	7,10,14,17	2,4,8,9,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	7,10,14,16,18	2,4,8,9,13,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	7,10,14,17,18	2,4,8,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	7,10,14,16	2,4,8,9,13,15	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	7,10,12,17,18	2,4,8,9,17,18	2^{-34}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	7,10,12,16	2,4,8,9	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	7,10,12,17	2,4,8,9,15,17	2^{-34}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	7,10,12,16,18	2,4,8,9,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	7,10,12,14	2,4,8,9	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	7,10,12,14,16,17,18	2,4,8,9,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	7,10,12,14,18	2,4,8,9,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	7,10,12,14,16,17	2,4,8,9,15,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	7,10,12,17	2,4,8,9,13,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	7,10,12,16,18	2,4,8,9,13,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	7,10,12,17,18	2,4,8,9,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	7,10,12,16	2,4,8,9,13,15	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	7,10,12,14,18	2,4,8,9,13,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	7,10,12,14,16,17	2,4,8,9,13,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	7,10,12,14	2,4,8,9,13,15	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	7,10,12,14,16,17,18	2,4,8,9,13,15,17,18	$2^{-28.5}$

Table 0.672 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	7,10,18	2,4,8,9,11,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	7,10,16,17	2,4,8,9,11,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	7,10	2,4,8,9,11,15	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	7,10,16,17,18	2,4,8,9,11,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	7,10,14,17	2,4,8,9,11,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	7,10,14,16,18	2,4,8,9,11,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	7,10,14,17,18	2,4,8,9,11,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	7,10,14,16	2,4,8,9,11,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	7,10	2,4,8,9,11,13	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	7,10,16,17,18	2,4,8,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	7,10,18	2,4,8,9,11,13,15,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	7,10,16,17	2,4,8,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	7,10,14,17,18	2,4,8,9,11,13,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	7,10,14,16	2,4,8,9,11,13	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	7,10,14,17	2,4,8,9,11,13,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	7,10,14,16,18	2,4,8,9,11,13,15,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	7,10,12,17	2,4,8,9,11,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	7,10,12,16,18	2,4,8,9,11,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	7,10,12,17,18	2,4,8,9,11,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	7,10,12,16	2,4,8,9,11,15	$2^{-6.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	7,10,12,14,18	2,4,8,9,11,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	7,10,12,14,16,17	2,4,8,9,11,17	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	7,10,12,14	2,4,8,9,11,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	7,10,12,14,16,17,18	2,4,8,9,11,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	7,10,12,17,18	2,4,8,9,11,13,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	7,10,12,16	2,4,8,9,11,13	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	7,10,12,17	2,4,8,9,11,13,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	7,10,12,16,18	2,4,8,9,11,13,15,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	7,10,12,14	2,4,8,9,11,13	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	7,10,12,14,16,17,18	2,4,8,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	7,10,12,14,18	2,4,8,9,11,13,15,18	2^{-12}
$(0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	7,10,12,14,16,17	2,4,8,9,11,13,15,17	$2^{-17.5}$

Table 0.673 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	17,18	2,4,6,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	16	2,4,6	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	17	2,4,6,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	16,18	2,4,6,15,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	14	2,4,6	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	14,16,17,18	2,4,6,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	14,18	2,4,6,15,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	14,16,17	2,4,6,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	17	2,4,6,13,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	16,18	2,4,6,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	17,18	2,4,6,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	16	2,4,6,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	14,18	2,4,6,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	14,16,17	2,4,6,13,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	14	2,4,6,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	14,16,17,18	2,4,6,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	12	2,4,6	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	12,16,17,18	2,4,6,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	12,18	2,4,6,15,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	12,16,17	2,4,6,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	12,14,17,18	2,4,6,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	12,14,16	2,4,6	2^{-34}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	12,14,17	2,4,6,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	12,14,16,18	2,4,6,15,18	2^{-34}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	12,18	2,4,6,13,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	12,16,17	2,4,6,13,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	12	2,4,6,13,15	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	12,16,17,18	2,4,6,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	12,14,17	2,4,6,13,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	12,14,16,18	2,4,6,13,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	12,14,17,18	2,4,6,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	12,14,16	2,4,6,13,15	$2^{-28.5}$

Table 0.674 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	17	2,4,6,11,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	16,18	2,4,6,11,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	17,18	2,4,6,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	16	2,4,6,11,15	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	14,18	2,4,6,11,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	14,16,17	2,4,6,11,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	14	2,4,6,11,15	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	14,16,17,18	2,4,6,11,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	17,18	2,4,6,11,13,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	16	2,4,6,11,13	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	17	2,4,6,11,13,15,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	16,18	2,4,6,11,13,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	14	2,4,6,11,13	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	14,16,17,18	2,4,6,11,13,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	14,18	2,4,6,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	14,16,17	2,4,6,11,13,15,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	12,18	2,4,6,11,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	12,16,17	2,4,6,11,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	12	2,4,6,11,15	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	12,16,17,18	2,4,6,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	12,14,17	2,4,6,11,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	12,14,16,18	2,4,6,11,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	12,14,17,18	2,4,6,11,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	12,14,16	2,4,6,11,15	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	12	2,4,6,11,13	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	12,16,17,18	2,4,6,11,13,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	12,18	2,4,6,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	12,16,17	2,4,6,11,13,15,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	12,14,17,18	2,4,6,11,13,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	12,14,16	2,4,6,11,13	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	12,14,17	2,4,6,11,13,15,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	12,14,16,18	2,4,6,11,13,15,18	$2^{-28.5}$

Table 0.675 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	10	2,4,6	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	10,16,17,18	2,4,6,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	10,18	2,4,6,15,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	10,16,17	2,4,6,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	10,14,17,18	2,4,6,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	10,14,16	2,4,6	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	10,14,17	2,4,6,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	10,14,16,18	2,4,6,15,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	10,18	2,4,6,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	10,16,17	2,4,6,13,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	10	2,4,6,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	10,16,17,18	2,4,6,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	10,14,17	2,4,6,13,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	10,14,16,18	2,4,6,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	10,14,17,18	2,4,6,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	10,14,16	2,4,6,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	10,12,17,18	2,4,6,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	10,12,16	2,4,6	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	10,12,17	2,4,6,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	10,12,16,18	2,4,6,15,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	10,12,14	2,4,6	2^{-1}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	10,12,14,16,17,18	2,4,6,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	10,12,14,18	2,4,6,15,18	2^{-1}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	10,12,14,16,17	2,4,6,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	10,12,17	2,4,6,13,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	10,12,16,18	2,4,6,13,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	10,12,17,18	2,4,6,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	10,12,16	2,4,6,13,15	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	10,12,14,18	2,4,6,13,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	10,12,14,16,17	2,4,6,13,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	10,12,14	2,4,6,13,15	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	10,12,14,16,17,18	2,4,6,13,15,17,18	2^{-23}

Table 0.676 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	10,18	2,4,6,11,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	10,16,17	2,4,6,11,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	10	2,4,6,11,15	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	10,16,17,18	2,4,6,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	10,14,17	2,4,6,11,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	10,14,16,18	2,4,6,11,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	10,14,17,18	2,4,6,11,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	10,14,16	2,4,6,11,15	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	10	2,4,6,11,13	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	10,16,17,18	2,4,6,11,13,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	10,18	2,4,6,11,13,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	10,16,17	2,4,6,11,13,15,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	10,14,17,18	2,4,6,11,13,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	10,14,16	2,4,6,11,13	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	10,14,17	2,4,6,11,13,15,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	10,14,16,18	2,4,6,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	10,12,17	2,4,6,11,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	10,12,16,18	2,4,6,11,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	10,12,17,18	2,4,6,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	10,12,16	2,4,6,11,15	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	10,12,14,18	2,4,6,11,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	10,12,14,16,17	2,4,6,11,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	10,12,14	2,4,6,11,15	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	10,12,14,16,17,18	2,4,6,11,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	10,12,17,18	2,4,6,11,13,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	10,12,16	2,4,6,11,13	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	10,12,17	2,4,6,11,13,15,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	10,12,16,18	2,4,6,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	10,12,14	2,4,6,11,13	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	10,12,14,16,17,18	2,4,6,11,13,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	10,12,14,18	2,4,6,11,13,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	10,12,14,16,17	2,4,6,11,13,15,17	2^{-23}

Table 0.677 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	17	2,4,6,9,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	16,18	2,4,6,9,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	17,18	2,4,6,9,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	16	2,4,6,9,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	14,18	2,4,6,9,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	14,16,17	2,4,6,9,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	14	2,4,6,9,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	14,16,17,18	2,4,6,9,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	17,18	2,4,6,9,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	16	2,4,6,9,13	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	17	2,4,6,9,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	16,18	2,4,6,9,13,15,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	14	2,4,6,9,13	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	14,16,17,18	2,4,6,9,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	14,18	2,4,6,9,13,15,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	14,16,17	2,4,6,9,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	12,18	2,4,6,9,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	12,16,17	2,4,6,9,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	12	2,4,6,9,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	12,16,17,18	2,4,6,9,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	12,14,17	2,4,6,9,17	2^{-1}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	12,14,16,18	2,4,6,9,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	12,14,17,18	2,4,6,9,15,17,18	2^{-1}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	12,14,16	2,4,6,9,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	12	2,4,6,9,13	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	12,16,17,18	2,4,6,9,13,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	12,18	2,4,6,9,13,15,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	12,16,17	2,4,6,9,13,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	12,14,17,18	2,4,6,9,13,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	12,14,16	2,4,6,9,13	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	12,14,17	2,4,6,9,13,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	12,14,16,18	2,4,6,9,13,15,18	2^{-23}

Table 0.678 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	17,18	2,4,6,9,11,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	16	2,4,6,9,11	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	17	2,4,6,9,11,15,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	16,18	2,4,6,9,11,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	14	2,4,6,9,11	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	14,16,17,18	2,4,6,9,11,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	14,18	2,4,6,9,11,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	14,16,17	2,4,6,9,11,15,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	17	2,4,6,9,11,13,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	16,18	2,4,6,9,11,13,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	17,18	2,4,6,9,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	16	2,4,6,9,11,13,15	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	14,18	2,4,6,9,11,13,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	14,16,17	2,4,6,9,11,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	14	2,4,6,9,11,13,15	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	14,16,17,18	2,4,6,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	12	2,4,6,9,11	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	12,16,17,18	2,4,6,9,11,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	12,18	2,4,6,9,11,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	12,16,17	2,4,6,9,11,15,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	12,14,17,18	2,4,6,9,11,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	12,14,16	2,4,6,9,11	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	12,14,17	2,4,6,9,11,15,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	12,14,16,18	2,4,6,9,11,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	12,18	2,4,6,9,11,13,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	12,16,17	2,4,6,9,11,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	12	2,4,6,9,11,13,15	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	12,16,17,18	2,4,6,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	12,14,17	2,4,6,9,11,13,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	12,14,16,18	2,4,6,9,11,13,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	12,14,17,18	2,4,6,9,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	12,14,16	2,4,6,9,11,13,15	2^{-23}

Table 0.679 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	10,18	2,4,6,9,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	10,16,17	2,4,6,9,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	10	2,4,6,9,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	10,16,17,18	2,4,6,9,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	10,14,17	2,4,6,9,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	10,14,16,18	2,4,6,9,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	10,14,17,18	2,4,6,9,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	10,14,16	2,4,6,9,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	10	2,4,6,9,13	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	10,16,17,18	2,4,6,9,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	10,18	2,4,6,9,13,15,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	10,16,17	2,4,6,9,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	10,14,17,18	2,4,6,9,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	10,14,16	2,4,6,9,13	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	10,14,17	2,4,6,9,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	10,14,16,18	2,4,6,9,13,15,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	10,12,17	2,4,6,9,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	10,12,16,18	2,4,6,9,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	10,12,17,18	2,4,6,9,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	10,12,16	2,4,6,9,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	10,12,14,18	2,4,6,9,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	10,12,14,16,17	2,4,6,9,17	2^{-34}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	10,12,14	2,4,6,9,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	10,12,14,16,17,18	2,4,6,9,15,17,18	2^{-34}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	10,12,17,18	2,4,6,9,13,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	10,12,16	2,4,6,9,13	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	10,12,17	2,4,6,9,13,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	10,12,16,18	2,4,6,9,13,15,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	10,12,14	2,4,6,9,13	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	10,12,14,16,17,18	2,4,6,9,13,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	10,12,14,18	2,4,6,9,13,15,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	10,12,14,16,17	2,4,6,9,13,15,17	$2^{-28.5}$

Table 0.680 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	10	2,4,6,9,11	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	10,16,17,18	2,4,6,9,11,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	10,18	2,4,6,9,11,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	10,16,17	2,4,6,9,11,15,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	10,14,17,18	2,4,6,9,11,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	10,14,16	2,4,6,9,11	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	10,14,17	2,4,6,9,11,15,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	10,14,16,18	2,4,6,9,11,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	10,18	2,4,6,9,11,13,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	10,16,17	2,4,6,9,11,13,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	10	2,4,6,9,11,13,15	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	10,16,17,18	2,4,6,9,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	10,14,17	2,4,6,9,11,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	10,14,16,18	2,4,6,9,11,13,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	10,14,17,18	2,4,6,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	10,14,16	2,4,6,9,11,13,15	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	10,12,17,18	2,4,6,9,11,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	10,12,16	2,4,6,9,11	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	10,12,17	2,4,6,9,11,15,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	10,12,16,18	2,4,6,9,11,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	10,12,14	2,4,6,9,11	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	10,12,14,16,17,18	2,4,6,9,11,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	10,12,14,18	2,4,6,9,11,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	10,12,14,16,17	2,4,6,9,11,15,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	10,12,17	2,4,6,9,11,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	10,12,16,18	2,4,6,9,11,13,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	10,12,17,18	2,4,6,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	10,12,16	2,4,6,9,11,13,15	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	10,12,14,18	2,4,6,9,11,13,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	10,12,14,16,17	2,4,6,9,11,13,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	10,12,14	2,4,6,9,11,13,15	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	10,12,14,16,17,18	2,4,6,9,11,13,15,17,18	$2^{-28.5}$

Table 0.681 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	—	2,4,6,8	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	16,17,18	2,4,6,8,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	18	2,4,6,8,15,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	16,17	2,4,6,8,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	14,17,18	2,4,6,8,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	14,16	2,4,6,8	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	14,17	2,4,6,8,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	14,16,18	2,4,6,8,15,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	18	2,4,6,8,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	16,17	2,4,6,8,13,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	—	2,4,6,8,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	16,17,18	2,4,6,8,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	14,17	2,4,6,8,13,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	14,16,18	2,4,6,8,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	14,17,18	2,4,6,8,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	14,16	2,4,6,8,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	12,17,18	2,4,6,8,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	12,16	2,4,6,8	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	12,17	2,4,6,8,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	12,16,18	2,4,6,8,15,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	12,14	2,4,6,8	2^{-34}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	12,14,16,17,18	2,4,6,8,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	12,14,18	2,4,6,8,15,18	2^{-34}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	12,14,16,17	2,4,6,8,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	12,17	2,4,6,8,13,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	12,16,18	2,4,6,8,13,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	12,17,18	2,4,6,8,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	12,16	2,4,6,8,13,15	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	12,14,18	2,4,6,8,13,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	12,14,16,17	2,4,6,8,13,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	12,14	2,4,6,8,13,15	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	12,14,16,17,18	2,4,6,8,13,15,17,18	2^{-12}

Table 0.682 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	18	2,4,6,8,11,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	16,17	2,4,6,8,11,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	—	2,4,6,8,11,15	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	16,17,18	2,4,6,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	14,17	2,4,6,8,11,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	14,16,18	2,4,6,8,11,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	14,17,18	2,4,6,8,11,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	14,16	2,4,6,8,11,15	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	—	2,4,6,8,11,13	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	16,17,18	2,4,6,8,11,13,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	18	2,4,6,8,11,13,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	16,17	2,4,6,8,11,13,15,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	14,17,18	2,4,6,8,11,13,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	14,16	2,4,6,8,11,13	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	14,17	2,4,6,8,11,13,15,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	14,16,18	2,4,6,8,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	12,17	2,4,6,8,11,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	12,16,18	2,4,6,8,11,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	12,17,18	2,4,6,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	12,16	2,4,6,8,11,15	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	12,14,18	2,4,6,8,11,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	12,14,16,17	2,4,6,8,11,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	12,14	2,4,6,8,11,15	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	12,14,16,17,18	2,4,6,8,11,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	12,17,18	2,4,6,8,11,13,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	12,16	2,4,6,8,11,13	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	12,17	2,4,6,8,11,13,15,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	12,16,18	2,4,6,8,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	12,14	2,4,6,8,11,13	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	12,14,16,17,18	2,4,6,8,11,13,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	12,14,18	2,4,6,8,11,13,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	12,14,16,17	2,4,6,8,11,13,15,17	2^{-12}

Table 0.683 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	10,17,18	2,4,6,8,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	10,16	2,4,6,8	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	10,17	2,4,6,8,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	10,16,18	2,4,6,8,15,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	10,14	2,4,6,8	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	10,14,16,17,18	2,4,6,8,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	10,14,18	2,4,6,8,15,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	10,14,16,17	2,4,6,8,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	10,17	2,4,6,8,13,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	10,16,18	2,4,6,8,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	10,17,18	2,4,6,8,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	10,16	2,4,6,8,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	10,14,18	2,4,6,8,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	10,14,16,17	2,4,6,8,13,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	10,14	2,4,6,8,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	10,14,16,17,18	2,4,6,8,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	10,12	2,4,6,8	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	10,12,16,17,18	2,4,6,8,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	10,12,18	2,4,6,8,15,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	10,12,16,17	2,4,6,8,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	10,12,14,17,18	2,4,6,8,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	10,12,14,16	2,4,6,8	2^{-1}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	10,12,14,17	2,4,6,8,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	10,12,14,16,18	2,4,6,8,15,18	2^{-1}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	10,12,18	2,4,6,8,13,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	10,12,16,17	2,4,6,8,13,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	10,12	2,4,6,8,13,15	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	10,12,16,17,18	2,4,6,8,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	10,12,14,17	2,4,6,8,13,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	10,12,14,16,18	2,4,6,8,13,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	10,12,14,17,18	2,4,6,8,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	10,12,14,16	2,4,6,8,13,15	$2^{-6.5}$

Table 0.684 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	10,17	2,4,6,8,11,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	10,16,18	2,4,6,8,11,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	10,17,18	2,4,6,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	10,16	2,4,6,8,11,15	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	10,14,18	2,4,6,8,11,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	10,14,16,17	2,4,6,8,11,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	10,14	2,4,6,8,11,15	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	10,14,16,17,18	2,4,6,8,11,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	10,17,18	2,4,6,8,11,13,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	10,16	2,4,6,8,11,13	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	10,17	2,4,6,8,11,13,15,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	10,16,18	2,4,6,8,11,13,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	10,14	2,4,6,8,11,13	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	10,14,16,17,18	2,4,6,8,11,13,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	10,14,18	2,4,6,8,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	10,14,16,17	2,4,6,8,11,13,15,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	10,12,18	2,4,6,8,11,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	10,12,16,17	2,4,6,8,11,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	10,12	2,4,6,8,11,15	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	10,12,16,17,18	2,4,6,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	10,12,14,17	2,4,6,8,11,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	10,12,14,16,18	2,4,6,8,11,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	10,12,14,17,18	2,4,6,8,11,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	10,12,14,16	2,4,6,8,11,15	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	10,12	2,4,6,8,11,13	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	10,12,16,17,18	2,4,6,8,11,13,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	10,12,18	2,4,6,8,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	10,12,16,17	2,4,6,8,11,13,15,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	10,12,14,17,18	2,4,6,8,11,13,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	10,12,14,16	2,4,6,8,11,13	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	10,12,14,17	2,4,6,8,11,13,15,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	10,12,14,16,18	2,4,6,8,11,13,15,18	$2^{-6.5}$

Table 0.685 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	18	2,4,6,8,9,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	16,17	2,4,6,8,9,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	—	2,4,6,8,9,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	16,17,18	2,4,6,8,9,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	14,17	2,4,6,8,9,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	14,16,18	2,4,6,8,9,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	14,17,18	2,4,6,8,9,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	14,16	2,4,6,8,9,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	—	2,4,6,8,9,13	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	16,17,18	2,4,6,8,9,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	18	2,4,6,8,9,13,15,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	16,17	2,4,6,8,9,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	14,17,18	2,4,6,8,9,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	14,16	2,4,6,8,9,13	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	14,17	2,4,6,8,9,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	14,16,18	2,4,6,8,9,13,15,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	12,17	2,4,6,8,9,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	12,16,18	2,4,6,8,9,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	12,17,18	2,4,6,8,9,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	12,16	2,4,6,8,9,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	12,14,18	2,4,6,8,9,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	12,14,16,17	2,4,6,8,9,17	2^{-1}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	12,14	2,4,6,8,9,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	12,14,16,17,18	2,4,6,8,9,15,17,18	2^{-1}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	12,17,18	2,4,6,8,9,13,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	12,16	2,4,6,8,9,13	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	12,17	2,4,6,8,9,13,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	12,16,18	2,4,6,8,9,13,15,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	12,14	2,4,6,8,9,13	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	12,14,16,17,18	2,4,6,8,9,13,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	12,14,18	2,4,6,8,9,13,15,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	12,14,16,17	2,4,6,8,9,13,15,17	$2^{-6.5}$

Table 0.686 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	—	2,4,6,8,9,11	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	16,17,18	2,4,6,8,9,11,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	18	2,4,6,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	16,17	2,4,6,8,9,11,15,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	14,17,18	2,4,6,8,9,11,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	14,16	2,4,6,8,9,11	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	14,17	2,4,6,8,9,11,15,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	14,16,18	2,4,6,8,9,11,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	18	2,4,6,8,9,11,13,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	16,17	2,4,6,8,9,11,13,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	—	2,4,6,8,9,11,13,15	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	16,17,18	2,4,6,8,9,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	14,17	2,4,6,8,9,11,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	14,16,18	2,4,6,8,9,11,13,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	14,17,18	2,4,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	14,16	2,4,6,8,9,11,13,15	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	12,17,18	2,4,6,8,9,11,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	12,16	2,4,6,8,9,11	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	12,17	2,4,6,8,9,11,15,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	12,16,18	2,4,6,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	12,14	2,4,6,8,9,11	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	12,14,16,17,18	2,4,6,8,9,11,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	12,14,18	2,4,6,8,9,11,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	12,14,16,17	2,4,6,8,9,11,15,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	12,17	2,4,6,8,9,11,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	12,16,18	2,4,6,8,9,11,13,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	12,17,18	2,4,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	12,16	2,4,6,8,9,11,13,15	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	12,14,18	2,4,6,8,9,11,13,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	12,14,16,17	2,4,6,8,9,11,13,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	12,14	2,4,6,8,9,11,13,15	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	12,14,16,17,18	2,4,6,8,9,11,13,15,17,18	$2^{-6.5}$

Table 0.687 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	10,17	2,4,6,8,9,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	10,16,18	2,4,6,8,9,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	10,17,18	2,4,6,8,9,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	10,16	2,4,6,8,9,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	10,14,18	2,4,6,8,9,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	10,14,16,17	2,4,6,8,9,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	10,14	2,4,6,8,9,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	10,14,16,17,18	2,4,6,8,9,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	10,17,18	2,4,6,8,9,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	10,16	2,4,6,8,9,13	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	10,17	2,4,6,8,9,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	10,16,18	2,4,6,8,9,13,15,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	10,14	2,4,6,8,9,13	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	10,14,16,17,18	2,4,6,8,9,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	10,14,18	2,4,6,8,9,13,15,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	10,14,16,17	2,4,6,8,9,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	10,12,18	2,4,6,8,9,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	10,12,16,17	2,4,6,8,9,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	10,12	2,4,6,8,9,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	10,12,16,17,18	2,4,6,8,9,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	10,12,14,17	2,4,6,8,9,17	2^{-34}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	10,12,14,16,18	2,4,6,8,9,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	10,12,14,17,18	2,4,6,8,9,15,17,18	2^{-34}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	10,12,14,16	2,4,6,8,9,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	10,12	2,4,6,8,9,13	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	10,12,16,17,18	2,4,6,8,9,13,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	10,12,18	2,4,6,8,9,13,15,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	10,12,16,17	2,4,6,8,9,13,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	10,12,14,17,18	2,4,6,8,9,13,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	10,12,14,16	2,4,6,8,9,13	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	10,12,14,17	2,4,6,8,9,13,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	10,12,14,16,18	2,4,6,8,9,13,15,18	2^{-12}

Table 0.688 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	10,17,18	2,4,6,8,9,11,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	10,16	2,4,6,8,9,11	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	10,17	2,4,6,8,9,11,15,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	10,16,18	2,4,6,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	10,14	2,4,6,8,9,11	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	10,14,16,17,18	2,4,6,8,9,11,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	10,14,18	2,4,6,8,9,11,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	10,14,16,17	2,4,6,8,9,11,15,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	10,17	2,4,6,8,9,11,13,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	10,16,18	2,4,6,8,9,11,13,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	10,17,18	2,4,6,8,9,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	10,16	2,4,6,8,9,11,13,15	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	10,14,18	2,4,6,8,9,11,13,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	10,14,16,17	2,4,6,8,9,11,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	10,14	2,4,6,8,9,11,13,15	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	10,14,16,17,18	2,4,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	10,12	2,4,6,8,9,11	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	10,12,16,17,18	2,4,6,8,9,11,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	10,12,18	2,4,6,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	10,12,16,17	2,4,6,8,9,11,15,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	10,12,14,17,18	2,4,6,8,9,11,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	10,12,14,16	2,4,6,8,9,11	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	10,12,14,17	2,4,6,8,9,11,15,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	10,12,14,16,18	2,4,6,8,9,11,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	10,12,18	2,4,6,8,9,11,13,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	10,12,16,17	2,4,6,8,9,11,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	10,12	2,4,6,8,9,11,13,15	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	10,12,16,17,18	2,4,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	10,12,14,17	2,4,6,8,9,11,13,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	10,12,14,16,18	2,4,6,8,9,11,13,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	10,12,14,17,18	2,4,6,8,9,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	10,12,14,16	2,4,6,8,9,11,13,15	2^{-12}

Table 0.689 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	7,17	2,4,6,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	7,16,18	2,4,6,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	7,17,18	2,4,6,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	7,16	2,4,6,15	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	7,14,18	2,4,6,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	7,14,16,17	2,4,6,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	7,14	2,4,6,15	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	7,14,16,17,18	2,4,6,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	7,17,18	2,4,6,13,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	7,16	2,4,6,13	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	7,17	2,4,6,13,15,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	7,16,18	2,4,6,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	7,14	2,4,6,13	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	7,14,16,17,18	2,4,6,13,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	7,14,18	2,4,6,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	7,14,16,17	2,4,6,13,15,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	7,12,18	2,4,6,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	7,12,16,17	2,4,6,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	7,12	2,4,6,15	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	7,12,16,17,18	2,4,6,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	7,12,14,17	2,4,6,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	7,12,14,16,18	2,4,6,18	2^{-34}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	7,12,14,17,18	2,4,6,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	7,12,14,16	2,4,6,15	2^{-34}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	7,12	2,4,6,13	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	7,12,16,17,18	2,4,6,13,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	7,12,18	2,4,6,13,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	7,12,16,17	2,4,6,13,15,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	7,12,14,17,18	2,4,6,13,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	7,12,14,16	2,4,6,13	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	7,12,14,17	2,4,6,13,15,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	7,12,14,16,18	2,4,6,13,15,18	$2^{-28.5}$

Table 0.690 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	7,17,18	2,4,6,11,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	7,16	2,4,6,11	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	7,17	2,4,6,11,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	7,16,18	2,4,6,11,15,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	7,14	2,4,6,11	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	7,14,16,17,18	2,4,6,11,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	7,14,18	2,4,6,11,15,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	7,14,16,17	2,4,6,11,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	7,17	2,4,6,11,13,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	7,16,18	2,4,6,11,13,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	7,17,18	2,4,6,11,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	7,16	2,4,6,11,13,15	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	7,14,18	2,4,6,11,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	7,14,16,17	2,4,6,11,13,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	7,14	2,4,6,11,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	7,14,16,17,18	2,4,6,11,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	7,12	2,4,6,11	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	7,12,16,17,18	2,4,6,11,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	7,12,18	2,4,6,11,15,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	7,12,16,17	2,4,6,11,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	7,12,14,17,18	2,4,6,11,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	7,12,14,16	2,4,6,11	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	7,12,14,17	2,4,6,11,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	7,12,14,16,18	2,4,6,11,15,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	7,12,18	2,4,6,11,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	7,12,16,17	2,4,6,11,13,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	7,12	2,4,6,11,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	7,12,16,17,18	2,4,6,11,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	7,12,14,17	2,4,6,11,13,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	7,12,14,16,18	2,4,6,11,13,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	7,12,14,17,18	2,4,6,11,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	7,12,14,16	2,4,6,11,13,15	$2^{-28.5}$

Table 0.691 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	7,10,18	2,4,6,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	7,10,16,17	2,4,6,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	7,10	2,4,6,15	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	7,10,16,17,18	2,4,6,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	7,10,14,17	2,4,6,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	7,10,14,16,18	2,4,6,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	7,10,14,17,18	2,4,6,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	7,10,14,16	2,4,6,15	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	7,10	2,4,6,13	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	7,10,16,17,18	2,4,6,13,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	7,10,18	2,4,6,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	7,10,16,17	2,4,6,13,15,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	7,10,14,17,18	2,4,6,13,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	7,10,14,16	2,4,6,13	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	7,10,14,17	2,4,6,13,15,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	7,10,14,16,18	2,4,6,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	7,10,12,17	2,4,6,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	7,10,12,16,18	2,4,6,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	7,10,12,17,18	2,4,6,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	7,10,12,16	2,4,6,15	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	7,10,12,14,18	2,4,6,18	2^{-1}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	7,10,12,14,16,17	2,4,6,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	7,10,12,14	2,4,6,15	2^{-1}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	7,10,12,14,16,17,18	2,4,6,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	7,10,12,17,18	2,4,6,13,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	7,10,12,16	2,4,6,13	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	7,10,12,17	2,4,6,13,15,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	7,10,12,16,18	2,4,6,13,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	7,10,12,14	2,4,6,13	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	7,10,12,14,16,17,18	2,4,6,13,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	7,10,12,14,18	2,4,6,13,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	7,10,12,14,16,17	2,4,6,13,15,17	2^{-23}

Table 0.692 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	7,10	2,4,6,11	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	7,10,16,17,18	2,4,6,11,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	7,10,18	2,4,6,11,15,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	7,10,16,17	2,4,6,11,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	7,10,14,17,18	2,4,6,11,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	7,10,14,16	2,4,6,11	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	7,10,14,17	2,4,6,11,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	7,10,14,16,18	2,4,6,11,15,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	7,10,18	2,4,6,11,13,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	7,10,16,17	2,4,6,11,13,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	7,10	2,4,6,11,13,15	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	7,10,16,17,18	2,4,6,11,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	7,10,14,17	2,4,6,11,13,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	7,10,14,16,18	2,4,6,11,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	7,10,14,17,18	2,4,6,11,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	7,10,14,16	2,4,6,11,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	7,10,12,17,18	2,4,6,11,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	7,10,12,16	2,4,6,11	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	7,10,12,17	2,4,6,11,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	7,10,12,16,18	2,4,6,11,15,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	7,10,12,14	2,4,6,11	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	7,10,12,14,16,17,18	2,4,6,11,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	7,10,12,14,18	2,4,6,11,15,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	7,10,12,14,16,17	2,4,6,11,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	7,10,12,17	2,4,6,11,13,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	7,10,12,16,18	2,4,6,11,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	7,10,12,17,18	2,4,6,11,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	7,10,12,16	2,4,6,11,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	7,10,12,14,18	2,4,6,11,13,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	7,10,12,14,16,17	2,4,6,11,13,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	7,10,12,14	2,4,6,11,13,15	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	7,10,12,14,16,17,18	2,4,6,11,13,15,17,18	2^{-23}

Table 0.693 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	7,17,18	2,4,6,9,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	7,16	2,4,6,9	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	7,17	2,4,6,9,15,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	7,16,18	2,4,6,9,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	7,14	2,4,6,9	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	7,14,16,17,18	2,4,6,9,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	7,14,18	2,4,6,9,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	7,14,16,17	2,4,6,9,15,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	7,17	2,4,6,9,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	7,16,18	2,4,6,9,13,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	7,17,18	2,4,6,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	7,16	2,4,6,9,13,15	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	7,14,18	2,4,6,9,13,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	7,14,16,17	2,4,6,9,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	7,14	2,4,6,9,13,15	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	7,14,16,17,18	2,4,6,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	7,12	2,4,6,9	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	7,12,16,17,18	2,4,6,9,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	7,12,18	2,4,6,9,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	7,12,16,17	2,4,6,9,15,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	7,12,14,17,18	2,4,6,9,17,18	2^{-1}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	7,12,14,16	2,4,6,9	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	7,12,14,17	2,4,6,9,15,17	2^{-1}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	7,12,14,16,18	2,4,6,9,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	7,12,18	2,4,6,9,13,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	7,12,16,17	2,4,6,9,13,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	7,12	2,4,6,9,13,15	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	7,12,16,17,18	2,4,6,9,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	7,12,14,17	2,4,6,9,13,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	7,12,14,16,18	2,4,6,9,13,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	7,12,14,17,18	2,4,6,9,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	7,12,14,16	2,4,6,9,13,15	2^{-23}

Table 0.694 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	7,17	2,4,6,9,11,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	7,16,18	2,4,6,9,11,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	7,17,18	2,4,6,9,11,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	7,16	2,4,6,9,11,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	7,14,18	2,4,6,9,11,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	7,14,16,17	2,4,6,9,11,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	7,14	2,4,6,9,11,15	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	7,14,16,17,18	2,4,6,9,11,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	7,17,18	2,4,6,9,11,13,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	7,16	2,4,6,9,11,13	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	7,17	2,4,6,9,11,13,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	7,16,18	2,4,6,9,11,13,15,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	7,14	2,4,6,9,11,13	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	7,14,16,17,18	2,4,6,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	7,14,18	2,4,6,9,11,13,15,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	7,14,16,17	2,4,6,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	7,12,18	2,4,6,9,11,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	7,12,16,17	2,4,6,9,11,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	7,12	2,4,6,9,11,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	7,12,16,17,18	2,4,6,9,11,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	7,12,14,17	2,4,6,9,11,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	7,12,14,16,18	2,4,6,9,11,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	7,12,14,17,18	2,4,6,9,11,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	7,12,14,16	2,4,6,9,11,15	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	7,12	2,4,6,9,11,13	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	7,12,16,17,18	2,4,6,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	7,12,18	2,4,6,9,11,13,15,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	7,12,16,17	2,4,6,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	7,12,14,17,18	2,4,6,9,11,13,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	7,12,14,16	2,4,6,9,11,13	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	7,12,14,17	2,4,6,9,11,13,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	7,12,14,16,18	2,4,6,9,11,13,15,18	2^{-23}

Table 0.695 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	7,10	2,4,6,9	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	7,10,16,17,18	2,4,6,9,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	7,10,18	2,4,6,9,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	7,10,16,17	2,4,6,9,15,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	7,10,14,17,18	2,4,6,9,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	7,10,14,16	2,4,6,9	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	7,10,14,17	2,4,6,9,15,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	7,10,14,16,18	2,4,6,9,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	7,10,18	2,4,6,9,13,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	7,10,16,17	2,4,6,9,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	7,10	2,4,6,9,13,15	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	7,10,16,17,18	2,4,6,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	7,10,14,17	2,4,6,9,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	7,10,14,16,18	2,4,6,9,13,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	7,10,14,17,18	2,4,6,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	7,10,14,16	2,4,6,9,13,15	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	7,10,12,17,18	2,4,6,9,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	7,10,12,16	2,4,6,9	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	7,10,12,17	2,4,6,9,15,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	7,10,12,16,18	2,4,6,9,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	7,10,12,14	2,4,6,9	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	7,10,12,14,16,17,18	2,4,6,9,17,18	2^{-34}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	7,10,12,14,18	2,4,6,9,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	7,10,12,14,16,17	2,4,6,9,15,17	2^{-34}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	7,10,12,17	2,4,6,9,13,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	7,10,12,16,18	2,4,6,9,13,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	7,10,12,17,18	2,4,6,9,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	7,10,12,16	2,4,6,9,13,15	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	7,10,12,14,18	2,4,6,9,13,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	7,10,12,14,16,17	2,4,6,9,13,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	7,10,12,14	2,4,6,9,13,15	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	7,10,12,14,16,17,18	2,4,6,9,13,15,17,18	$2^{-28.5}$

Table 0.696 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	7,10,18	2,4,6,9,11,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	7,10,16,17	2,4,6,9,11,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	7,10	2,4,6,9,11,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	7,10,16,17,18	2,4,6,9,11,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	7,10,14,17	2,4,6,9,11,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	7,10,14,16,18	2,4,6,9,11,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	7,10,14,17,18	2,4,6,9,11,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	7,10,14,16	2,4,6,9,11,15	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	7,10	2,4,6,9,11,13	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	7,10,16,17,18	2,4,6,9,11,13,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	7,10,18	2,4,6,9,11,13,15,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	7,10,16,17	2,4,6,9,11,13,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	7,10,14,17,18	2,4,6,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	7,10,14,16	2,4,6,9,11,13	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	7,10,14,17	2,4,6,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	7,10,14,16,18	2,4,6,9,11,13,15,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	7,10,12,17	2,4,6,9,11,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	7,10,12,16,18	2,4,6,9,11,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	7,10,12,17,18	2,4,6,9,11,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	7,10,12,16	2,4,6,9,11,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	7,10,12,14,18	2,4,6,9,11,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	7,10,12,14,16,17	2,4,6,9,11,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	7,10,12,14	2,4,6,9,11,15	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	7,10,12,14,16,17,18	2,4,6,9,11,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	7,10,12,17,18	2,4,6,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	7,10,12,16	2,4,6,9,11,13	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	7,10,12,17	2,4,6,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	7,10,12,16,18	2,4,6,9,11,13,15,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	7,10,12,14	2,4,6,9,11,13	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	7,10,12,14,16,17,18	2,4,6,9,11,13,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	7,10,12,14,18	2,4,6,9,11,13,15,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	7,10,12,14,16,17	2,4,6,9,11,13,15,17	$2^{-28.5}$

Table 0.697 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	7,18	2,4,6,8,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	7,16,17	2,4,6,8,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	7	2,4,6,8,15	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	7,16,17,18	2,4,6,8,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	7,14,17	2,4,6,8,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	7,14,16,18	2,4,6,8,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	7,14,17,18	2,4,6,8,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	7,14,16	2,4,6,8,15	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	7	2,4,6,8,13	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	7,16,17,18	2,4,6,8,13,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	7,18	2,4,6,8,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	7,16,17	2,4,6,8,13,15,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	7,14,17,18	2,4,6,8,13,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	7,14,16	2,4,6,8,13	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	7,14,17	2,4,6,8,13,15,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	7,14,16,18	2,4,6,8,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	7,12,17	2,4,6,8,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	7,12,16,18	2,4,6,8,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	7,12,17,18	2,4,6,8,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	7,12,16	2,4,6,8,15	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	7,12,14,18	2,4,6,8,18	2^{-34}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	7,12,14,16,17	2,4,6,8,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	7,12,14	2,4,6,8,15	2^{-34}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	7,12,14,16,17,18	2,4,6,8,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	7,12,17,18	2,4,6,8,13,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	7,12,16	2,4,6,8,13	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	7,12,17	2,4,6,8,13,15,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	7,12,16,18	2,4,6,8,13,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	7,12,14	2,4,6,8,13	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	7,12,14,16,17,18	2,4,6,8,13,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	7,12,14,18	2,4,6,8,13,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	7,12,14,16,17	2,4,6,8,13,15,17	2^{-12}

Table 0.698 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	7	2,4,6,8,11	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	7,16,17,18	2,4,6,8,11,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	7,18	2,4,6,8,11,15,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	7,16,17	2,4,6,8,11,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	7,14,17,18	2,4,6,8,11,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	7,14,16	2,4,6,8,11	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	7,14,17	2,4,6,8,11,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	7,14,16,18	2,4,6,8,11,15,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	7,18	2,4,6,8,11,13,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	7,16,17	2,4,6,8,11,13,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	7	2,4,6,8,11,13,15	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	7,16,17,18	2,4,6,8,11,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	7,14,17	2,4,6,8,11,13,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	7,14,16,18	2,4,6,8,11,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	7,14,17,18	2,4,6,8,11,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	7,14,16	2,4,6,8,11,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	7,12,17,18	2,4,6,8,11,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	7,12,16	2,4,6,8,11	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	7,12,17	2,4,6,8,11,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	7,12,16,18	2,4,6,8,11,15,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	7,12,14	2,4,6,8,11	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	7,12,14,16,17,18	2,4,6,8,11,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	7,12,14,18	2,4,6,8,11,15,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	7,12,14,16,17	2,4,6,8,11,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	7,12,17	2,4,6,8,11,13,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	7,12,16,18	2,4,6,8,11,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	7,12,17,18	2,4,6,8,11,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	7,12,16	2,4,6,8,11,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	7,12,14,18	2,4,6,8,11,13,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	7,12,14,16,17	2,4,6,8,11,13,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	7,12,14	2,4,6,8,11,13,15	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	7,12,14,16,17,18	2,4,6,8,11,13,15,17,18	2^{-12}

Table 0.699 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	7,10,17	2,4,6,8,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	7,10,16,18	2,4,6,8,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	7,10,17,18	2,4,6,8,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	7,10,16	2,4,6,8,15	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	7,10,14,18	2,4,6,8,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	7,10,14,16,17	2,4,6,8,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	7,10,14	2,4,6,8,15	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	7,10,14,16,17,18	2,4,6,8,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	7,10,17,18	2,4,6,8,13,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	7,10,16	2,4,6,8,13	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	7,10,17	2,4,6,8,13,15,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	7,10,16,18	2,4,6,8,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	7,10,14	2,4,6,8,13	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	7,10,14,16,17,18	2,4,6,8,13,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	7,10,14,18	2,4,6,8,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	7,10,14,16,17	2,4,6,8,13,15,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	7,10,12,18	2,4,6,8,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	7,10,12,16,17	2,4,6,8,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	7,10,12	2,4,6,8,15	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	7,10,12,16,17,18	2,4,6,8,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	7,10,12,14,17	2,4,6,8,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	7,10,12,14,16,18	2,4,6,8,18	2^{-1}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	7,10,12,14,17,18	2,4,6,8,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	7,10,12,14,16	2,4,6,8,15	2^{-1}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	7,10,12	2,4,6,8,13	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	7,10,12,16,17,18	2,4,6,8,13,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	7,10,12,18	2,4,6,8,13,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	7,10,12,16,17	2,4,6,8,13,15,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	7,10,12,14,17,18	2,4,6,8,13,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	7,10,12,14,16	2,4,6,8,13	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	7,10,12,14,17	2,4,6,8,13,15,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	7,10,12,14,16,18	2,4,6,8,13,15,18	$2^{-6.5}$

Table 0.700 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	7,10,17,18	2,4,6,8,11,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	7,10,16	2,4,6,8,11	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	7,10,17	2,4,6,8,11,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	7,10,16,18	2,4,6,8,11,15,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	7,10,14	2,4,6,8,11	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	7,10,14,16,17,18	2,4,6,8,11,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	7,10,14,18	2,4,6,8,11,15,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	7,10,14,16,17	2,4,6,8,11,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	7,10,17	2,4,6,8,11,13,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	7,10,16,18	2,4,6,8,11,13,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	7,10,17,18	2,4,6,8,11,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	7,10,16	2,4,6,8,11,13,15	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	7,10,14,18	2,4,6,8,11,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	7,10,14,16,17	2,4,6,8,11,13,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	7,10,14	2,4,6,8,11,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	7,10,14,16,17,18	2,4,6,8,11,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	7,10,12	2,4,6,8,11	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	7,10,12,16,17,18	2,4,6,8,11,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	7,10,12,18	2,4,6,8,11,15,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	7,10,12,16,17	2,4,6,8,11,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	7,10,12,14,17,18	2,4,6,8,11,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	7,10,12,14,16	2,4,6,8,11	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	7,10,12,14,17	2,4,6,8,11,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	7,10,12,14,16,18	2,4,6,8,11,15,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	7,10,12,18	2,4,6,8,11,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	7,10,12,16,17	2,4,6,8,11,13,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	7,10,12	2,4,6,8,11,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	7,10,12,16,17,18	2,4,6,8,11,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	7,10,12,14,17	2,4,6,8,11,13,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	7,10,12,14,16,18	2,4,6,8,11,13,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	7,10,12,14,17,18	2,4,6,8,11,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	7,10,12,14,16	2,4,6,8,11,13,15	$2^{-6.5}$

Table 0.701 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	7	2,4,6,8,9	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	7,16,17,18	2,4,6,8,9,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	7,18	2,4,6,8,9,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	7,16,17	2,4,6,8,9,15,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	7,14,17,18	2,4,6,8,9,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	7,14,16	2,4,6,8,9	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	7,14,17	2,4,6,8,9,15,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	7,14,16,18	2,4,6,8,9,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	7,18	2,4,6,8,9,13,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	7,16,17	2,4,6,8,9,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	7	2,4,6,8,9,13,15	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	7,16,17,18	2,4,6,8,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	7,14,17	2,4,6,8,9,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	7,14,16,18	2,4,6,8,9,13,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	7,14,17,18	2,4,6,8,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	7,14,16	2,4,6,8,9,13,15	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	7,12,17,18	2,4,6,8,9,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	7,12,16	2,4,6,8,9	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	7,12,17	2,4,6,8,9,15,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	7,12,16,18	2,4,6,8,9,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	7,12,14	2,4,6,8,9	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	7,12,14,16,17,18	2,4,6,8,9,17,18	2^{-1}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	7,12,14,18	2,4,6,8,9,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	7,12,14,16,17	2,4,6,8,9,15,17	2^{-1}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	7,12,17	2,4,6,8,9,13,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	7,12,16,18	2,4,6,8,9,13,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	7,12,17,18	2,4,6,8,9,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	7,12,16	2,4,6,8,9,13,15	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	7,12,14,18	2,4,6,8,9,13,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	7,12,14,16,17	2,4,6,8,9,13,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	7,12,14	2,4,6,8,9,13,15	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	7,12,14,16,17,18	2,4,6,8,9,13,15,17,18	$2^{-6.5}$

Table 0.702 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	7,18	2,4,6,8,9,11,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	7,16,17	2,4,6,8,9,11,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	7	2,4,6,8,9,11,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	7,16,17,18	2,4,6,8,9,11,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	7,14,17	2,4,6,8,9,11,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	7,14,16,18	2,4,6,8,9,11,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	7,14,17,18	2,4,6,8,9,11,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	7,14,16	2,4,6,8,9,11,15	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	7	2,4,6,8,9,11,13	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	7,16,17,18	2,4,6,8,9,11,13,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	7,18	2,4,6,8,9,11,13,15,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	7,16,17	2,4,6,8,9,11,13,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	7,14,17,18	2,4,6,8,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	7,14,16	2,4,6,8,9,11,13	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	7,14,17	2,4,6,8,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	7,14,16,18	2,4,6,8,9,11,13,15,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	7,12,17	2,4,6,8,9,11,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	7,12,16,18	2,4,6,8,9,11,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	7,12,17,18	2,4,6,8,9,11,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	7,12,16	2,4,6,8,9,11,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	7,12,14,18	2,4,6,8,9,11,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	7,12,14,16,17	2,4,6,8,9,11,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	7,12,14	2,4,6,8,9,11,15	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	7,12,14,16,17,18	2,4,6,8,9,11,15,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	7,12,17,18	2,4,6,8,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	7,12,16	2,4,6,8,9,11,13	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	7,12,17	2,4,6,8,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	7,12,16,18	2,4,6,8,9,11,13,15,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	7,12,14	2,4,6,8,9,11,13	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	7,12,14,16,17,18	2,4,6,8,9,11,13,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	7,12,14,18	2,4,6,8,9,11,13,15,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	7,12,14,16,17	2,4,6,8,9,11,13,15,17	$2^{-6.5}$

Table 0.703 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	7,10,17,18	2,4,6,8,9,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	7,10,16	2,4,6,8,9	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	7,10,17	2,4,6,8,9,15,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	7,10,16,18	2,4,6,8,9,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	7,10,14	2,4,6,8,9	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	7,10,14,16,17,18	2,4,6,8,9,17,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	7,10,14,18	2,4,6,8,9,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	7,10,14,16,17	2,4,6,8,9,15,17	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	7,10,17	2,4,6,8,9,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	7,10,16,18	2,4,6,8,9,13,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	7,10,17,18	2,4,6,8,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	7,10,16	2,4,6,8,9,13,15	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	7,10,14,18	2,4,6,8,9,13,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	7,10,14,16,17	2,4,6,8,9,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	7,10,14	2,4,6,8,9,13,15	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	7,10,14,16,17,18	2,4,6,8,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	7,10,12	2,4,6,8,9	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	7,10,12,16,17,18	2,4,6,8,9,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	7,10,12,18	2,4,6,8,9,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	7,10,12,16,17	2,4,6,8,9,15,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	7,10,12,14,17,18	2,4,6,8,9,17,18	2^{-34}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	7,10,12,14,16	2,4,6,8,9	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	7,10,12,14,17	2,4,6,8,9,15,17	2^{-34}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	7,10,12,14,16,18	2,4,6,8,9,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	7,10,12,18	2,4,6,8,9,13,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	7,10,12,16,17	2,4,6,8,9,13,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	7,10,12	2,4,6,8,9,13,15	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	7,10,12,16,17,18	2,4,6,8,9,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	7,10,12,14,17	2,4,6,8,9,13,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	7,10,12,14,16,18	2,4,6,8,9,13,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	7,10,12,14,17,18	2,4,6,8,9,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	7,10,12,14,16	2,4,6,8,9,13,15	2^{-12}

Table 0.704 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	7,10,17	2,4,6,8,9,11,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	7,10,16,18	2,4,6,8,9,11,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	7,10,17,18	2,4,6,8,9,11,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	7,10,16	2,4,6,8,9,11,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	7,10,14,18	2,4,6,8,9,11,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	7,10,14,16,17	2,4,6,8,9,11,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	7,10,14	2,4,6,8,9,11,15	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	7,10,14,16,17,18	2,4,6,8,9,11,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	7,10,17,18	2,4,6,8,9,11,13,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	7,10,16	2,4,6,8,9,11,13	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	7,10,17	2,4,6,8,9,11,13,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	7,10,16,18	2,4,6,8,9,11,13,15,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	7,10,14	2,4,6,8,9,11,13	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	7,10,14,16,17,18	2,4,6,8,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	7,10,14,18	2,4,6,8,9,11,13,15,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	7,10,14,16,17	2,4,6,8,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	7,10,12,18	2,4,6,8,9,11,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	7,10,12,16,17	2,4,6,8,9,11,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	7,10,12	2,4,6,8,9,11,15	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	7,10,12,16,17,18	2,4,6,8,9,11,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	7,10,12,14,17	2,4,6,8,9,11,17	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	7,10,12,14,16,18	2,4,6,8,9,11,18	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	7,10,12,14,17,18	2,4,6,8,9,11,15,17,18	2^{-23}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	7,10,12,14,16	2,4,6,8,9,11,15	$2^{-6.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	7,10,12	2,4,6,8,9,11,13	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	7,10,12,16,17,18	2,4,6,8,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	7,10,12,18	2,4,6,8,9,11,13,15,18	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	7,10,12,16,17	2,4,6,8,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	7,10,12,14,17,18	2,4,6,8,9,11,13,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	7,10,12,14,16	2,4,6,8,9,11,13	2^{-12}
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	7,10,12,14,17	2,4,6,8,9,11,13,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	7,10,12,14,16,18	2,4,6,8,9,11,13,15,18	2^{-12}

Table 0.705 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(2)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	5,18	2,4,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	5,16,17	2,4,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	5	2,4,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	5,16,17,18	2,4,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	5,14,17	2,4,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	5,14,16,18	2,4,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	5,14,17,18	2,4,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	5,14,16	2,4,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	5	2,4,13	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	5,16,17,18	2,4,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	5,18	2,4,13,15,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	5,16,17	2,4,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	5,14,17,18	2,4,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	5,14,16	2,4,13	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	5,14,17	2,4,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	5,14,16,18	2,4,13,15,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	5,12,17	2,4,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	5,12,16,18	2,4,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	5,12,17,18	2,4,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	5,12,16	2,4,15	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	5,12,14,18	2,4,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	5,12,14,16,17	2,4,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	5,12,14	2,4,15	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	5,12,14,16,17,18	2,4,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	5,12,17,18	2,4,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	5,12,16	2,4,13	2^{-34}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	5,12,17	2,4,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	5,12,16,18	2,4,13,15,18	2^{-34}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	5,12,14	2,4,13	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	5,12,14,16,17,18	2,4,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	5,12,14,18	2,4,13,15,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	5,12,14,16,17	2,4,13,15,17	$2^{-17.5}$

Table 0.706 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	5	2,4,11	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	5,16,17,18	2,4,11,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	5,18	2,4,11,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	5,16,17	2,4,11,15,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	5,14,17,18	2,4,11,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	5,14,16	2,4,11	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	5,14,17	2,4,11,15,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	5,14,16,18	2,4,11,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	5,18	2,4,11,13,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	5,16,17	2,4,11,13,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	5	2,4,11,13,15	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	5,16,17,18	2,4,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	5,14,17	2,4,11,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	5,14,16,18	2,4,11,13,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	5,14,17,18	2,4,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	5,14,16	2,4,11,13,15	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	5,12,17,18	2,4,11,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	5,12,16	2,4,11	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	5,12,17	2,4,11,15,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	5,12,16,18	2,4,11,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	5,12,14	2,4,11	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	5,12,14,16,17,18	2,4,11,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	5,12,14,18	2,4,11,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	5,12,14,16,17	2,4,11,15,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	5,12,17	2,4,11,13,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	5,12,16,18	2,4,11,13,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	5,12,17,18	2,4,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	5,12,16	2,4,11,13,15	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	5,12,14,18	2,4,11,13,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	5,12,14,16,17	2,4,11,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	5,12,14	2,4,11,13,15	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	5,12,14,16,17,18	2,4,11,13,15,17,18	$2^{-17.5}$

Table 0.707 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(2)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	5,10,17	2,4,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	5,10,16,18	2,4,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	5,10,17,18	2,4,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	5,10,16	2,4,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	5,10,14,18	2,4,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	5,10,14,16,17	2,4,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	5,10,14	2,4,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	5,10,14,16,17,18	2,4,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	5,10,17,18	2,4,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	5,10,16	2,4,13	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	5,10,17	2,4,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	5,10,16,18	2,4,13,15,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	5,10,14	2,4,13	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	5,10,14,16,17,18	2,4,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	5,10,14,18	2,4,13,15,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	5,10,14,16,17	2,4,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	5,10,12,18	2,4,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	5,10,12,16,17	2,4,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	5,10,12	2,4,15	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	5,10,12,16,17,18	2,4,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	5,10,12,14,17	2,4,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	5,10,12,14,16,18	2,4,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	5,10,12,14,17,18	2,4,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	5,10,12,14,16	2,4,15	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	5,10,12	2,4,13	2^{-1}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	5,10,12,16,17,18	2,4,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	5,10,12,18	2,4,13,15,18	2^{-1}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	5,10,12,16,17	2,4,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	5,10,12,14,17,18	2,4,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	5,10,12,14,16	2,4,13	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	5,10,12,14,17	2,4,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	5,10,12,14,16,18	2,4,13,15,18	2^{-12}

Table 0.708 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	5,10,17,18	2,4,11,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	5,10,16	2,4,11	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	5,10,17	2,4,11,15,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	5,10,16,18	2,4,11,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	5,10,14	2,4,11	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	5,10,14,16,17,18	2,4,11,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	5,10,14,18	2,4,11,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	5,10,14,16,17	2,4,11,15,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	5,10,17	2,4,11,13,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	5,10,16,18	2,4,11,13,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	5,10,17,18	2,4,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	5,10,16	2,4,11,13,15	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	5,10,14,18	2,4,11,13,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	5,10,14,16,17	2,4,11,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	5,10,14	2,4,11,13,15	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	5,10,14,16,17,18	2,4,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	5,10,12	2,4,11	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	5,10,12,16,17,18	2,4,11,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	5,10,12,18	2,4,11,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	5,10,12,16,17	2,4,11,15,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	5,10,12,14,17,18	2,4,11,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	5,10,12,14,16	2,4,11	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	5,10,12,14,17	2,4,11,15,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	5,10,12,14,16,18	2,4,11,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	5,10,12,18	2,4,11,13,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	5,10,12,16,17	2,4,11,13,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	5,10,12	2,4,11,13,15	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	5,10,12,16,17,18	2,4,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	5,10,12,14,17	2,4,11,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	5,10,12,14,16,18	2,4,11,13,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	5,10,12,14,17,18	2,4,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	5,10,12,14,16	2,4,11,13,15	2^{-12}

Table 0.709 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	5	2,4,9	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	5,16,17,18	2,4,9,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	5,18	2,4,9,15,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	5,16,17	2,4,9,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	5,14,17,18	2,4,9,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	5,14,16	2,4,9	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	5,14,17	2,4,9,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	5,14,16,18	2,4,9,15,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	5,18	2,4,9,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	5,16,17	2,4,9,13,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	5	2,4,9,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	5,16,17,18	2,4,9,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	5,14,17	2,4,9,13,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	5,14,16,18	2,4,9,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	5,14,17,18	2,4,9,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	5,14,16	2,4,9,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	5,12,17,18	2,4,9,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	5,12,16	2,4,9	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	5,12,17	2,4,9,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	5,12,16,18	2,4,9,15,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	5,12,14	2,4,9	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	5,12,14,16,17,18	2,4,9,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	5,12,14,18	2,4,9,15,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	5,12,14,16,17	2,4,9,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	5,12,17	2,4,9,13,17	2^{-1}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	5,12,16,18	2,4,9,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	5,12,17,18	2,4,9,13,15,17,18	2^{-1}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	5,12,16	2,4,9,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	5,12,14,18	2,4,9,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	5,12,14,16,17	2,4,9,13,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	5,12,14	2,4,9,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	5,12,14,16,17,18	2,4,9,13,15,17,18	2^{-12}

Table 0.710 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	5,18	2,4,9,11,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	5,16,17	2,4,9,11,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	5	2,4,9,11,15	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	5,16,17,18	2,4,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	5,14,17	2,4,9,11,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	5,14,16,18	2,4,9,11,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	5,14,17,18	2,4,9,11,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	5,14,16	2,4,9,11,15	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	5	2,4,9,11,13	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	5,16,17,18	2,4,9,11,13,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	5,18	2,4,9,11,13,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	5,16,17	2,4,9,11,13,15,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	5,14,17,18	2,4,9,11,13,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	5,14,16	2,4,9,11,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	5,14,17	2,4,9,11,13,15,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	5,14,16,18	2,4,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	5,12,17	2,4,9,11,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	5,12,16,18	2,4,9,11,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	5,12,17,18	2,4,9,11,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	5,12,16	2,4,9,11,15	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	5,12,14,18	2,4,9,11,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	5,12,14,16,17	2,4,9,11,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	5,12,14	2,4,9,11,15	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	5,12,14,16,17,18	2,4,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	5,12,17,18	2,4,9,11,13,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	5,12,16	2,4,9,11,13	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	5,12,17	2,4,9,11,13,15,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	5,12,16,18	2,4,9,11,13,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	5,12,14	2,4,9,11,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	5,12,14,16,17,18	2,4,9,11,13,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	5,12,14,18	2,4,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	5,12,14,16,17	2,4,9,11,13,15,17	2^{-12}

Table 0.711 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	5,10,17,18	2,4,9,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	5,10,16	2,4,9	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	5,10,17	2,4,9,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	5,10,16,18	2,4,9,15,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	5,10,14	2,4,9	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	5,10,14,16,17,18	2,4,9,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	5,10,14,18	2,4,9,15,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	5,10,14,16,17	2,4,9,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	5,10,17	2,4,9,13,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	5,10,16,18	2,4,9,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	5,10,17,18	2,4,9,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	5,10,16	2,4,9,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	5,10,14,18	2,4,9,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	5,10,14,16,17	2,4,9,13,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	5,10,14	2,4,9,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	5,10,14,16,17,18	2,4,9,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	5,10,12	2,4,9	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	5,10,12,16,17,18	2,4,9,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	5,10,12,18	2,4,9,15,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	5,10,12,16,17	2,4,9,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	5,10,12,14,17,18	2,4,9,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	5,10,12,14,16	2,4,9	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	5,10,12,14,17	2,4,9,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	5,10,12,14,16,18	2,4,9,15,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	5,10,12,18	2,4,9,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	5,10,12,16,17	2,4,9,13,17	2^{-34}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	5,10,12	2,4,9,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	5,10,12,16,17,18	2,4,9,13,15,17,18	2^{-34}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	5,10,12,14,17	2,4,9,13,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	5,10,12,14,16,18	2,4,9,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	5,10,12,14,17,18	2,4,9,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	5,10,12,14,16	2,4,9,13,15	$2^{-17.5}$

Table 0.712 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	5,10,17	2,4,9,11,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	5,10,16,18	2,4,9,11,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	5,10,17,18	2,4,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	5,10,16	2,4,9,11,15	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	5,10,14,18	2,4,9,11,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	5,10,14,16,17	2,4,9,11,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	5,10,14	2,4,9,11,15	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	5,10,14,16,17,18	2,4,9,11,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	5,10,17,18	2,4,9,11,13,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	5,10,16	2,4,9,11,13	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	5,10,17	2,4,9,11,13,15,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	5,10,16,18	2,4,9,11,13,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	5,10,14	2,4,9,11,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	5,10,14,16,17,18	2,4,9,11,13,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	5,10,14,18	2,4,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	5,10,14,16,17	2,4,9,11,13,15,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	5,10,12,18	2,4,9,11,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	5,10,12,16,17	2,4,9,11,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	5,10,12	2,4,9,11,15	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	5,10,12,16,17,18	2,4,9,11,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	5,10,12,14,17	2,4,9,11,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	5,10,12,14,16,18	2,4,9,11,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	5,10,12,14,17,18	2,4,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	5,10,12,14,16	2,4,9,11,15	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	5,10,12	2,4,9,11,13	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	5,10,12,16,17,18	2,4,9,11,13,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	5,10,12,18	2,4,9,11,13,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	5,10,12,16,17	2,4,9,11,13,15,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	5,10,12,14,17,18	2,4,9,11,13,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	5,10,12,14,16	2,4,9,11,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	5,10,12,14,17	2,4,9,11,13,15,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	5,10,12,14,16,18	2,4,9,11,13,15,18	$2^{-17.5}$

Table 0.713 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	5,17	2,4,8,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	5,16,18	2,4,8,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	5,17,18	2,4,8,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	5,16	2,4,8,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	5,14,18	2,4,8,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	5,14,16,17	2,4,8,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	5,14	2,4,8,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	5,14,16,17,18	2,4,8,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	5,17,18	2,4,8,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	5,16	2,4,8,13	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	5,17	2,4,8,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	5,16,18	2,4,8,13,15,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	5,14	2,4,8,13	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	5,14,16,17,18	2,4,8,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	5,14,18	2,4,8,13,15,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	5,14,16,17	2,4,8,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	5,12,18	2,4,8,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	5,12,16,17	2,4,8,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	5,12	2,4,8,15	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	5,12,16,17,18	2,4,8,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	5,12,14,17	2,4,8,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	5,12,14,16,18	2,4,8,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	5,12,14,17,18	2,4,8,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	5,12,14,16	2,4,8,15	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	5,12	2,4,8,13	2^{-34}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	5,12,16,17,18	2,4,8,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	5,12,18	2,4,8,13,15,18	2^{-34}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	5,12,16,17	2,4,8,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	5,12,14,17,18	2,4,8,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	5,12,14,16	2,4,8,13	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	5,12,14,17	2,4,8,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	5,12,14,16,18	2,4,8,13,15,18	2^{-23}

Table 0.714 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	5,17,18	2,4,8,11,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	5,16	2,4,8,11	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	5,17	2,4,8,11,15,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	5,16,18	2,4,8,11,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	5,14	2,4,8,11	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	5,14,16,17,18	2,4,8,11,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	5,14,18	2,4,8,11,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	5,14,16,17	2,4,8,11,15,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	5,17	2,4,8,11,13,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	5,16,18	2,4,8,11,13,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	5,17,18	2,4,8,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	5,16	2,4,8,11,13,15	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	5,14,18	2,4,8,11,13,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	5,14,16,17	2,4,8,11,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	5,14	2,4,8,11,13,15	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	5,14,16,17,18	2,4,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	5,12	2,4,8,11	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	5,12,16,17,18	2,4,8,11,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	5,12,18	2,4,8,11,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	5,12,16,17	2,4,8,11,15,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	5,12,14,17,18	2,4,8,11,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	5,12,14,16	2,4,8,11	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	5,12,14,17	2,4,8,11,15,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	5,12,14,16,18	2,4,8,11,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	5,12,18	2,4,8,11,13,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	5,12,16,17	2,4,8,11,13,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	5,12	2,4,8,11,13,15	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	5,12,16,17,18	2,4,8,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	5,12,14,17	2,4,8,11,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	5,12,14,16,18	2,4,8,11,13,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	5,12,14,17,18	2,4,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	5,12,14,16	2,4,8,11,13,15	2^{-23}

Table 0.715 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	5,10,18	2,4,8,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	5,10,16,17	2,4,8,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	5,10	2,4,8,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	5,10,16,17,18	2,4,8,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	5,10,14,17	2,4,8,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	5,10,14,16,18	2,4,8,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	5,10,14,17,18	2,4,8,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	5,10,14,16	2,4,8,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	5,10	2,4,8,13	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	5,10,16,17,18	2,4,8,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	5,10,18	2,4,8,13,15,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	5,10,16,17	2,4,8,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	5,10,14,17,18	2,4,8,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	5,10,14,16	2,4,8,13	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	5,10,14,17	2,4,8,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	5,10,14,16,18	2,4,8,13,15,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	5,10,12,17	2,4,8,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	5,10,12,16,18	2,4,8,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	5,10,12,16	2,4,8,15	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	5,10,12,14,18	2,4,8,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	5,10,12,14,16,17	2,4,8,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	5,10,12,14	2,4,8,15	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	5,10,12,14,16,17,18	2,4,8,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	5,10,12,17,18	2,4,8,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	5,10,12,16	2,4,8,13	2^{-1}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	5,10,12,17	2,4,8,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	5,10,12,16,18	2,4,8,13,15,18	2^{-1}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	5,10,12,14	2,4,8,13	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	5,10,12,14,16,17,18	2,4,8,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	5,10,12,14,18	2,4,8,13,15,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	5,10,12,14,16,17	2,4,8,13,15,17	$2^{-17.5}$

Table 0.716 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	5,10	2,4,8,11	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	5,10,16,17,18	2,4,8,11,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	5,10,18	2,4,8,11,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	5,10,16,17	2,4,8,11,15,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	5,10,14,17,18	2,4,8,11,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	5,10,14,16	2,4,8,11	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	5,10,14,17	2,4,8,11,15,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	5,10,14,16,18	2,4,8,11,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	5,10,18	2,4,8,11,13,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	5,10,16,17	2,4,8,11,13,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	5,10	2,4,8,11,13,15	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	5,10,16,17,18	2,4,8,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	5,10,14,17	2,4,8,11,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	5,10,14,16,18	2,4,8,11,13,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	5,10,14,17,18	2,4,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	5,10,14,16	2,4,8,11,13,15	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	5,10,12,17,18	2,4,8,11,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	5,10,12,16	2,4,8,11	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	5,10,12,17	2,4,8,11,15,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	5,10,12,16,18	2,4,8,11,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	5,10,12,14	2,4,8,11	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	5,10,12,14,16,17,18	2,4,8,11,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	5,10,12,14,18	2,4,8,11,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	5,10,12,14,16,17	2,4,8,11,15,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	5,10,12,17	2,4,8,11,13,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	5,10,12,16,18	2,4,8,11,13,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	5,10,12,17,18	2,4,8,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	5,10,12,16	2,4,8,11,13,15	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	5,10,12,14,18	2,4,8,11,13,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	5,10,12,14,16,17	2,4,8,11,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	5,10,12,14	2,4,8,11,13,15	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	5,10,12,14,16,17,18	2,4,8,11,13,15,17,18	$2^{-17.5}$

Table 0.717 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	5,17,18	2,4,8,9,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	5,16	2,4,8,9	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	5,17	2,4,8,9,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	5,16,18	2,4,8,9,15,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	5,14	2,4,8,9	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	5,14,16,17,18	2,4,8,9,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	5,14,18	2,4,8,9,15,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	5,14,16,17	2,4,8,9,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	5,17	2,4,8,9,13,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	5,16,18	2,4,8,9,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	5,17,18	2,4,8,9,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	5,16	2,4,8,9,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	5,14,18	2,4,8,9,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	5,14,16,17	2,4,8,9,13,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	5,14	2,4,8,9,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	5,14,16,17,18	2,4,8,9,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	5,12	2,4,8,9	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	5,12,16,17,18	2,4,8,9,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	5,12,18	2,4,8,9,15,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	5,12,16,17	2,4,8,9,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	5,12,14,17,18	2,4,8,9,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	5,12,14,16	2,4,8,9	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	5,12,14,17	2,4,8,9,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	5,12,14,16,18	2,4,8,9,15,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	5,12,18	2,4,8,9,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	5,12,16,17	2,4,8,9,13,17	2^{-1}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	5,12	2,4,8,9,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	5,12,16,17,18	2,4,8,9,13,15,17,18	2^{-1}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	5,12,14,17	2,4,8,9,13,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	5,12,14,16,18	2,4,8,9,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	5,12,14,17,18	2,4,8,9,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	5,12,14,16	2,4,8,9,13,15	$2^{-17.5}$

Table 0.718 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	5,17	2,4,8,9,11,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	5,16,18	2,4,8,9,11,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	5,17,18	2,4,8,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	5,16	2,4,8,9,11,15	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	5,14,18	2,4,8,9,11,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	5,14,16,17	2,4,8,9,11,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	5,14	2,4,8,9,11,15	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	5,14,16,17,18	2,4,8,9,11,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	5,17,18	2,4,8,9,11,13,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	5,16	2,4,8,9,11,13	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	5,17	2,4,8,9,11,13,15,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	5,16,18	2,4,8,9,11,13,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	5,14	2,4,8,9,11,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	5,14,16,17,18	2,4,8,9,11,13,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	5,14,18	2,4,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	5,14,16,17	2,4,8,9,11,13,15,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	5,12,18	2,4,8,9,11,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	5,12,16,17	2,4,8,9,11,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	5,12	2,4,8,9,11,15	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	5,12,16,17,18	2,4,8,9,11,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	5,12,14,17	2,4,8,9,11,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	5,12,14,16,18	2,4,8,9,11,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	5,12,14,17,18	2,4,8,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	5,12,14,16	2,4,8,9,11,15	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	5,12	2,4,8,9,11,13	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	5,12,16,17,18	2,4,8,9,11,13,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	5,12,18	2,4,8,9,11,13,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	5,12,16,17	2,4,8,9,11,13,15,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	5,12,14,17,18	2,4,8,9,11,13,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	5,12,14,16	2,4,8,9,11,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	5,12,14,17	2,4,8,9,11,13,15,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	5,12,14,16,18	2,4,8,9,11,13,15,18	$2^{-17.5}$

Table 0.719 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	5,10	2,4,8,9	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	5,10,16,17,18	2,4,8,9,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	5,10,18	2,4,8,9,15,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	5,10,16,17	2,4,8,9,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	5,10,14,17,18	2,4,8,9,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	5,10,14,16	2,4,8,9	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	5,10,14,17	2,4,8,9,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	5,10,14,16,18	2,4,8,9,15,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	5,10,18	2,4,8,9,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	5,10,16,17	2,4,8,9,13,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	5,10	2,4,8,9,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	5,10,16,17,18	2,4,8,9,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	5,10,14,17	2,4,8,9,13,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	5,10,14,16,18	2,4,8,9,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	5,10,14,17,18	2,4,8,9,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	5,10,14,16	2,4,8,9,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	5,10,12,17,18	2,4,8,9,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	5,10,12,16	2,4,8,9	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	5,10,12,17	2,4,8,9,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	5,10,12,16,18	2,4,8,9,15,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	5,10,12,14	2,4,8,9	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	5,10,12,14,16,17,18	2,4,8,9,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	5,10,12,14,18	2,4,8,9,15,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	5,10,12,14,16,17	2,4,8,9,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	5,10,12,17	2,4,8,9,13,17	2^{-34}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	5,10,12,16,18	2,4,8,9,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	5,10,12,17,18	2,4,8,9,13,15,17,18	2^{-34}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	5,10,12,16	2,4,8,9,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	5,10,12,14,18	2,4,8,9,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	5,10,12,14,16,17	2,4,8,9,13,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	5,10,12,14	2,4,8,9,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	5,10,12,14,16,17,18	2,4,8,9,13,15,17,18	2^{-23}

Table 0.720 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	5,10,18	2,4,8,9,11,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	5,10,16,17	2,4,8,9,11,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	5,10	2,4,8,9,11,15	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	5,10,16,17,18	2,4,8,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	5,10,14,17	2,4,8,9,11,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	5,10,14,16,18	2,4,8,9,11,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	5,10,14,17,18	2,4,8,9,11,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	5,10,14,16	2,4,8,9,11,15	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	5,10	2,4,8,9,11,13	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	5,10,16,17,18	2,4,8,9,11,13,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	5,10,18	2,4,8,9,11,13,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	5,10,16,17	2,4,8,9,11,13,15,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	5,10,14,17,18	2,4,8,9,11,13,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	5,10,14,16	2,4,8,9,11,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	5,10,14,17	2,4,8,9,11,13,15,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	5,10,14,16,18	2,4,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	5,10,12,17	2,4,8,9,11,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	5,10,12,16,18	2,4,8,9,11,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	5,10,12,17,18	2,4,8,9,11,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	5,10,12,16	2,4,8,9,11,15	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	5,10,12,14,18	2,4,8,9,11,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	5,10,12,14,16,17	2,4,8,9,11,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	5,10,12,14	2,4,8,9,11,15	2^{-12}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	5,10,12,14,16,17,18	2,4,8,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	5,10,12,17,18	2,4,8,9,11,13,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	5,10,12,16	2,4,8,9,11,13	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	5,10,12,17	2,4,8,9,11,13,15,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	5,10,12,16,18	2,4,8,9,11,13,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	5,10,12,14	2,4,8,9,11,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	5,10,12,14,16,17,18	2,4,8,9,11,13,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	5,10,12,14,18	2,4,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	5,10,12,14,16,17	2,4,8,9,11,13,15,17	2^{-23}

Table 0.721 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	5,7	2,4	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	5,7,16,17,18	2,4,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	5,7,18	2,4,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	5,7,16,17	2,4,15,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	5,7,14,17,18	2,4,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	5,7,14,16	2,4	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	5,7,14,17	2,4,15,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	5,7,14,16,18	2,4,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	5,7,18	2,4,13,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	5,7,16,17	2,4,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	5,7	2,4,13,15	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	5,7,16,17,18	2,4,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	5,7,14,17	2,4,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	5,7,14,16,18	2,4,13,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	5,7,14,17,18	2,4,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	5,7,14,16	2,4,13,15	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	5,7,12,17,18	2,4,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	5,7,12,16	2,4	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	5,7,12,17	2,4,15,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	5,7,12,16,18	2,4,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	5,7,12,14	2,4	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	5,7,12,14,16,17,18	2,4,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	5,7,12,14,18	2,4,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	5,7,12,14,16,17	2,4,15,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	5,7,12,17	2,4,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	5,7,12,16,18	2,4,13,18	2^{-34}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	5,7,12,17,18	2,4,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	5,7,12,16	2,4,13,15	2^{-34}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	5,7,12,14,18	2,4,13,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	5,7,12,14,16,17	2,4,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	5,7,12,14	2,4,13,15	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	5,7,12,14,16,17,18	2,4,13,15,17,18	$2^{-17.5}$

Table 0.722 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	5,7,18	2,4,11,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	5,7,16,17	2,4,11,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	5,7	2,4,11,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	5,7,16,17,18	2,4,11,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	5,7,14,17	2,4,11,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	5,7,14,16,18	2,4,11,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	5,7,14,17,18	2,4,11,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	5,7,14,16	2,4,11,15	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	5,7	2,4,11,13	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	5,7,16,17,18	2,4,11,13,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	5,7,18	2,4,11,13,15,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	5,7,16,17	2,4,11,13,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	5,7,14,17,18	2,4,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	5,7,14,16	2,4,11,13	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	5,7,14,17	2,4,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	5,7,14,16,18	2,4,11,13,15,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	5,7,12,17	2,4,11,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	5,7,12,16,18	2,4,11,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	5,7,12,17,18	2,4,11,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	5,7,12,16	2,4,11,15	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	5,7,12,14,18	2,4,11,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	5,7,12,14,16,17	2,4,11,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	5,7,12,14	2,4,11,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	5,7,12,14,16,17,18	2,4,11,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	5,7,12,17,18	2,4,11,13,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	5,7,12,16	2,4,11,13	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	5,7,12,17	2,4,11,13,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	5,7,12,16,18	2,4,11,13,15,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	5,7,12,14	2,4,11,13	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	5,7,12,14,16,17,18	2,4,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	5,7,12,14,18	2,4,11,13,15,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	5,7,12,14,16,17	2,4,11,13,15,17	$2^{-17.5}$

Table 0.723 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	5,7,10,17,18	2,4,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	5,7,10,16	2,4	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	5,7,10,17	2,4,15,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	5,7,10,16,18	2,4,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	5,7,10,14	2,4	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	5,7,10,14,16,17,18	2,4,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	5,7,10,14,18	2,4,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	5,7,10,14,16,17	2,4,15,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	5,7,10,17	2,4,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	5,7,10,16,18	2,4,13,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	5,7,10,17,18	2,4,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	5,7,10,16	2,4,13,15	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	5,7,10,14,18	2,4,13,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	5,7,10,14,16,17	2,4,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	5,7,10,14	2,4,13,15	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	5,7,10,14,16,17,18	2,4,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	5,7,10,12	2,4	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	5,7,10,12,16,17,18	2,4,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	5,7,10,12,18	2,4,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	5,7,10,12,16,17	2,4,15,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	5,7,10,12,14,17,18	2,4,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	5,7,10,12,14,16	2,4	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	5,7,10,12,14,17	2,4,15,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	5,7,10,12,14,16,18	2,4,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	5,7,10,12,18	2,4,13,18	2^{-1}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	5,7,10,12,16,17	2,4,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	5,7,10,12	2,4,13,15	2^{-1}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	5,7,10,12,16,17,18	2,4,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	5,7,10,12,14,17	2,4,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	5,7,10,12,14,16,18	2,4,13,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	5,7,10,12,14,17,18	2,4,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	5,7,10,12,14,16	2,4,13,15	2^{-12}

Table 0.724 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	5,7,10,17	2,4,11,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	5,7,10,16,18	2,4,11,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	5,7,10,17,18	2,4,11,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	5,7,10,16	2,4,11,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	5,7,10,14,18	2,4,11,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	5,7,10,14,16,17	2,4,11,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	5,7,10,14	2,4,11,15	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	5,7,10,14,16,17,18	2,4,11,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	5,7,10,17,18	2,4,11,13,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	5,7,10,16	2,4,11,13	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	5,7,10,17	2,4,11,13,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	5,7,10,16,18	2,4,11,13,15,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	5,7,10,14	2,4,11,13	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	5,7,10,14,16,17,18	2,4,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	5,7,10,14,18	2,4,11,13,15,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	5,7,10,14,16,17	2,4,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	5,7,10,12,18	2,4,11,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	5,7,10,12,16,17	2,4,11,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	5,7,10,12	2,4,11,15	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	5,7,10,12,16,17,18	2,4,11,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	5,7,10,12,14,17	2,4,11,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	5,7,10,12,14,16,18	2,4,11,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	5,7,10,12,14,17,18	2,4,11,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	5,7,10,12,14,16	2,4,11,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	5,7,10,12	2,4,11,13	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	5,7,10,12,16,17,18	2,4,11,13,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	5,7,10,12,18	2,4,11,13,15,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	5,7,10,12,16,17	2,4,11,13,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	5,7,10,12,14,17,18	2,4,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	5,7,10,12,14,16	2,4,11,13	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	5,7,10,12,14,17	2,4,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	5,7,10,12,14,16,18	2,4,11,13,15,18	2^{-12}

Table 0.725 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	5,7,18	2,4,9,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	5,7,16,17	2,4,9,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	5,7	2,4,9,15	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	5,7,16,17,18	2,4,9,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	5,7,14,17	2,4,9,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	5,7,14,16,18	2,4,9,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	5,7,14,17,18	2,4,9,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	5,7,14,16	2,4,9,15	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	5,7	2,4,9,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	5,7,16,17,18	2,4,9,13,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	5,7,18	2,4,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	5,7,16,17	2,4,9,13,15,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	5,7,14,17,18	2,4,9,13,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	5,7,14,16	2,4,9,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	5,7,14,17	2,4,9,13,15,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	5,7,14,16,18	2,4,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	5,7,12,17	2,4,9,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	5,7,12,16,18	2,4,9,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	5,7,12,17,18	2,4,9,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	5,7,12,16	2,4,9,15	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	5,7,12,14,18	2,4,9,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	5,7,12,14,16,17	2,4,9,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	5,7,12,14	2,4,9,15	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	5,7,12,14,16,17,18	2,4,9,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	5,7,12,17,18	2,4,9,13,17,18	2^{-1}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	5,7,12,16	2,4,9,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	5,7,12,17	2,4,9,13,15,17	2^{-1}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	5,7,12,16,18	2,4,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	5,7,12,14	2,4,9,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	5,7,12,14,16,17,18	2,4,9,13,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	5,7,12,14,18	2,4,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	5,7,12,14,16,17	2,4,9,13,15,17	2^{-12}

Table 0.726 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	5,7	2,4,9,11	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	5,7,16,17,18	2,4,9,11,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	5,7,18	2,4,9,11,15,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	5,7,16,17	2,4,9,11,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	5,7,14,17,18	2,4,9,11,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	5,7,14,16	2,4,9,11	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	5,7,14,17	2,4,9,11,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	5,7,14,16,18	2,4,9,11,15,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	5,7,18	2,4,9,11,13,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	5,7,16,17	2,4,9,11,13,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	5,7	2,4,9,11,13,15	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	5,7,16,17,18	2,4,9,11,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	5,7,14,17	2,4,9,11,13,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	5,7,14,16,18	2,4,9,11,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	5,7,14,17,18	2,4,9,11,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	5,7,14,16	2,4,9,11,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	5,7,12,17,18	2,4,9,11,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	5,7,12,16	2,4,9,11	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	5,7,12,17	2,4,9,11,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	5,7,12,16,18	2,4,9,11,15,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	5,7,12,14	2,4,9,11	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	5,7,12,14,16,17,18	2,4,9,11,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	5,7,12,14,18	2,4,9,11,15,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	5,7,12,14,16,17	2,4,9,11,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	5,7,12,17	2,4,9,11,13,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	5,7,12,16,18	2,4,9,11,13,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	5,7,12,17,18	2,4,9,11,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	5,7,12,16	2,4,9,11,13,15	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	5,7,12,14,18	2,4,9,11,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	5,7,12,14,16,17	2,4,9,11,13,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	5,7,12,14	2,4,9,11,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	5,7,12,14,16,17,18	2,4,9,11,13,15,17,18	2^{-12}

Table 0.727 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	5,7,10,17	2,4,9,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	5,7,10,16,18	2,4,9,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	5,7,10,17,18	2,4,9,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	5,7,10,16	2,4,9,15	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	5,7,10,14,18	2,4,9,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	5,7,10,14,16,17	2,4,9,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	5,7,10,14	2,4,9,15	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	5,7,10,14,16,17,18	2,4,9,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	5,7,10,17,18	2,4,9,13,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	5,7,10,16	2,4,9,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	5,7,10,17	2,4,9,13,15,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	5,7,10,16,18	2,4,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	5,7,10,14	2,4,9,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	5,7,10,14,16,17,18	2,4,9,13,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	5,7,10,14,18	2,4,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	5,7,10,14,16,17	2,4,9,13,15,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	5,7,10,12,18	2,4,9,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	5,7,10,12,16,17	2,4,9,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	5,7,10,12	2,4,9,15	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	5,7,10,12,16,17,18	2,4,9,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	5,7,10,12,14,17	2,4,9,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	5,7,10,12,14,16,18	2,4,9,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	5,7,10,12,14,17,18	2,4,9,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	5,7,10,12,14,16	2,4,9,15	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	5,7,10,12	2,4,9,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	5,7,10,12,16,17,18	2,4,9,13,17,18	2^{-34}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	5,7,10,12,18	2,4,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	5,7,10,12,16,17	2,4,9,13,15,17	2^{-34}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	5,7,10,12,14,17,18	2,4,9,13,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	5,7,10,12,14,16	2,4,9,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	5,7,10,12,14,17	2,4,9,13,15,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	5,7,10,12,14,16,18	2,4,9,13,15,18	$2^{-17.5}$

Table 0.728 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	5,7,10,17,18	2,4,9,11,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	5,7,10,16	2,4,9,11	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	5,7,10,17	2,4,9,11,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	5,7,10,16,18	2,4,9,11,15,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	5,7,10,14	2,4,9,11	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	5,7,10,14,16,17,18	2,4,9,11,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	5,7,10,14,18	2,4,9,11,15,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	5,7,10,14,16,17	2,4,9,11,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	5,7,10,17	2,4,9,11,13,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	5,7,10,16,18	2,4,9,11,13,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	5,7,10,17,18	2,4,9,11,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	5,7,10,16	2,4,9,11,13,15	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	5,7,10,14,18	2,4,9,11,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	5,7,10,14,16,17	2,4,9,11,13,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	5,7,10,14	2,4,9,11,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	5,7,10,14,16,17,18	2,4,9,11,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	5,7,10,12	2,4,9,11	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	5,7,10,12,16,17,18	2,4,9,11,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	5,7,10,12,18	2,4,9,11,15,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	5,7,10,12,16,17	2,4,9,11,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	5,7,10,12,14,17,18	2,4,9,11,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	5,7,10,12,14,16	2,4,9,11	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	5,7,10,12,14,17	2,4,9,11,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	5,7,10,12,14,16,18	2,4,9,11,15,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	5,7,10,12,18	2,4,9,11,13,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	5,7,10,12,16,17	2,4,9,11,13,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	5,7,10,12	2,4,9,11,13,15	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	5,7,10,12,16,17,18	2,4,9,11,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	5,7,10,12,14,17	2,4,9,11,13,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	5,7,10,12,14,16,18	2,4,9,11,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	5,7,10,12,14,17,18	2,4,9,11,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	5,7,10,12,14,16	2,4,9,11,13,15	$2^{-17.5}$

Table 0.729 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	5,7,17,18	2,4,8,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	5,7,16	2,4,8	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	5,7,17	2,4,8,15,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	5,7,16,18	2,4,8,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	5,7,14	2,4,8	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	5,7,14,16,17,18	2,4,8,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	5,7,14,18	2,4,8,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	5,7,14,16,17	2,4,8,15,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	5,7,17	2,4,8,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	5,7,16,18	2,4,8,13,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	5,7,17,18	2,4,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	5,7,16	2,4,8,13,15	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	5,7,14,18	2,4,8,13,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	5,7,14,16,17	2,4,8,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	5,7,14	2,4,8,13,15	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	5,7,14,16,17,18	2,4,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	5,7,12	2,4,8	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	5,7,12,16,17,18	2,4,8,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	5,7,12,18	2,4,8,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	5,7,12,16,17	2,4,8,15,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	5,7,12,14,17,18	2,4,8,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	5,7,12,14,16	2,4,8	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	5,7,12,14,17	2,4,8,15,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	5,7,12,14,16,18	2,4,8,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	5,7,12,18	2,4,8,13,18	2^{-34}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	5,7,12,16,17	2,4,8,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	5,7,12	2,4,8,13,15	2^{-34}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	5,7,12,16,17,18	2,4,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	5,7,12,14,17	2,4,8,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	5,7,12,14,16,18	2,4,8,13,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	5,7,12,14,17,18	2,4,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	5,7,12,14,16	2,4,8,13,15	2^{-23}

Table 0.730 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	5,7,17	2,4,8,11,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	5,7,16,18	2,4,8,11,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	5,7,17,18	2,4,8,11,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	5,7,16	2,4,8,11,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	5,7,14,18	2,4,8,11,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	5,7,14,16,17	2,4,8,11,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	5,7,14	2,4,8,11,15	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	5,7,14,16,17,18	2,4,8,11,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	5,7,17,18	2,4,8,11,13,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	5,7,16	2,4,8,11,13	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	5,7,17	2,4,8,11,13,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	5,7,16,18	2,4,8,11,13,15,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	5,7,14	2,4,8,11,13	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	5,7,14,16,17,18	2,4,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	5,7,14,18	2,4,8,11,13,15,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	5,7,14,16,17	2,4,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	5,7,12,18	2,4,8,11,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	5,7,12,16,17	2,4,8,11,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	5,7,12	2,4,8,11,15	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	5,7,12,16,17,18	2,4,8,11,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	5,7,12,14,17	2,4,8,11,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	5,7,12,14,16,18	2,4,8,11,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	5,7,12,14,17,18	2,4,8,11,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	5,7,12,14,16	2,4,8,11,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	5,7,12	2,4,8,11,13	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	5,7,12,16,17,18	2,4,8,11,13,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	5,7,12,18	2,4,8,11,13,15,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	5,7,12,16,17	2,4,8,11,13,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	5,7,12,14,17,18	2,4,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	5,7,12,14,16	2,4,8,11,13	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	5,7,12,14,17	2,4,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	5,7,12,14,16,18	2,4,8,11,13,15,18	2^{-23}

Table 0.731 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	5,7,10	2,4,8	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	5,7,10,16,17,18	2,4,8,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	5,7,10,18	2,4,8,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	5,7,10,16,17	2,4,8,15,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	5,7,10,14,17,18	2,4,8,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	5,7,10,14,16	2,4,8	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	5,7,10,14,17	2,4,8,15,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	5,7,10,14,16,18	2,4,8,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	5,7,10,18	2,4,8,13,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	5,7,10,16,17	2,4,8,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	5,7,10	2,4,8,13,15	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	5,7,10,16,17,18	2,4,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	5,7,10,14,17	2,4,8,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	5,7,10,14,16,18	2,4,8,13,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	5,7,10,14,17,18	2,4,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	5,7,10,14,16	2,4,8,13,15	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	5,7,10,12,17,18	2,4,8,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	5,7,10,12,16	2,4,8	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	5,7,10,12,17	2,4,8,15,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	5,7,10,12,16,18	2,4,8,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	5,7,10,12,14	2,4,8	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	5,7,10,12,14,16,17,18	2,4,8,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	5,7,10,12,14,18	2,4,8,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	5,7,10,12,14,16,17	2,4,8,15,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	5,7,10,12,17	2,4,8,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	5,7,10,12,16,18	2,4,8,13,18	2^{-1}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	5,7,10,12,17,18	2,4,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	5,7,10,12,16	2,4,8,13,15	2^{-1}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	5,7,10,12,14,18	2,4,8,13,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	5,7,10,12,14,16,17	2,4,8,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	5,7,10,12,14	2,4,8,13,15	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	5,7,10,12,14,16,17,18	2,4,8,13,15,17,18	$2^{-17.5}$

Table 0.732 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	5,7,10,18	2,4,8,11,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	5,7,10,16,17	2,4,8,11,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	5,7,10	2,4,8,11,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	5,7,10,16,17,18	2,4,8,11,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	5,7,10,14,17	2,4,8,11,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	5,7,10,14,16,18	2,4,8,11,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	5,7,10,14,17,18	2,4,8,11,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	5,7,10,14,16	2,4,8,11,15	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	5,7,10	2,4,8,11,13	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	5,7,10,16,17,18	2,4,8,11,13,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	5,7,10,18	2,4,8,11,13,15,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	5,7,10,16,17	2,4,8,11,13,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	5,7,10,14,17,18	2,4,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	5,7,10,14,16	2,4,8,11,13	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	5,7,10,14,17	2,4,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	5,7,10,14,16,18	2,4,8,11,13,15,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	5,7,10,12,17	2,4,8,11,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	5,7,10,12,16,18	2,4,8,11,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	5,7,10,12,17,18	2,4,8,11,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	5,7,10,12,16	2,4,8,11,15	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	5,7,10,12,14,18	2,4,8,11,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	5,7,10,12,14,16,17	2,4,8,11,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	5,7,10,12,14	2,4,8,11,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	5,7,10,12,14,16,17,18	2,4,8,11,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	5,7,10,12,17,18	2,4,8,11,13,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	5,7,10,12,16	2,4,8,11,13	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	5,7,10,12,17	2,4,8,11,13,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	5,7,10,12,16,18	2,4,8,11,13,15,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	5,7,10,12,14	2,4,8,11,13	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	5,7,10,12,14,16,17,18	2,4,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	5,7,10,12,14,18	2,4,8,11,13,15,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	5,7,10,12,14,16,17	2,4,8,11,13,15,17	$2^{-17.5}$

Table 0.733 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	5,7,17	2,4,8,9,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	5,7,16,18	2,4,8,9,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	5,7,17,18	2,4,8,9,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	5,7,16	2,4,8,9,15	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	5,7,14,18	2,4,8,9,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	5,7,14,16,17	2,4,8,9,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	5,7,14	2,4,8,9,15	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	5,7,14,16,17,18	2,4,8,9,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	5,7,17,18	2,4,8,9,13,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	5,7,16	2,4,8,9,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	5,7,17	2,4,8,9,13,15,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	5,7,16,18	2,4,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	5,7,14	2,4,8,9,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	5,7,14,16,17,18	2,4,8,9,13,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	5,7,14,18	2,4,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	5,7,14,16,17	2,4,8,9,13,15,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	5,7,12,18	2,4,8,9,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	5,7,12,16,17	2,4,8,9,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	5,7,12	2,4,8,9,15	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	5,7,12,16,17,18	2,4,8,9,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	5,7,12,14,17	2,4,8,9,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	5,7,12,14,16,18	2,4,8,9,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	5,7,12,14,17,18	2,4,8,9,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	5,7,12,14,16	2,4,8,9,15	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	5,7,12	2,4,8,9,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	5,7,12,16,17,18	2,4,8,9,13,17,18	2^{-1}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	5,7,12,18	2,4,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	5,7,12,16,17	2,4,8,9,13,15,17	2^{-1}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	5,7,12,14,17,18	2,4,8,9,13,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	5,7,12,14,16	2,4,8,9,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	5,7,12,14,17	2,4,8,9,13,15,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	5,7,12,14,16,18	2,4,8,9,13,15,18	$2^{-17.5}$

Table 0.734 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	5,7,17,18	2,4,8,9,11,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	5,7,16	2,4,8,9,11	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	5,7,17	2,4,8,9,11,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	5,7,16,18	2,4,8,9,11,15,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	5,7,14	2,4,8,9,11	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	5,7,14,16,17,18	2,4,8,9,11,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	5,7,14,18	2,4,8,9,11,15,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	5,7,14,16,17	2,4,8,9,11,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	5,7,17	2,4,8,9,11,13,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	5,7,16,18	2,4,8,9,11,13,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	5,7,17,18	2,4,8,9,11,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	5,7,16	2,4,8,9,11,13,15	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	5,7,14,18	2,4,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	5,7,14,16,17	2,4,8,9,11,13,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	5,7,14	2,4,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	5,7,14,16,17,18	2,4,8,9,11,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	5,7,12	2,4,8,9,11	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	5,7,12,16,17,18	2,4,8,9,11,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	5,7,12,18	2,4,8,9,11,15,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	5,7,12,16,17	2,4,8,9,11,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	5,7,12,14,17,18	2,4,8,9,11,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	5,7,12,14,16	2,4,8,9,11	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	5,7,12,14,17	2,4,8,9,11,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	5,7,12,14,16,18	2,4,8,9,11,15,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	5,7,12,18	2,4,8,9,11,13,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	5,7,12,16,17	2,4,8,9,11,13,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	5,7,12	2,4,8,9,11,13,15	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	5,7,12,16,17,18	2,4,8,9,11,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	5,7,12,14,17	2,4,8,9,11,13,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	5,7,12,14,16,18	2,4,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	5,7,12,14,17,18	2,4,8,9,11,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	5,7,12,14,16	2,4,8,9,11,13,15	$2^{-17.5}$

Table 0.735 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	5,7,10,18	2,4,8,9,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	5,7,10,16,17	2,4,8,9,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	5,7,10	2,4,8,9,15	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	5,7,10,16,17,18	2,4,8,9,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	5,7,10,14,17	2,4,8,9,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	5,7,10,14,16,18	2,4,8,9,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	5,7,10,14,17,18	2,4,8,9,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	5,7,10,14,16	2,4,8,9,15	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	5,7,10	2,4,8,9,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	5,7,10,16,17,18	2,4,8,9,13,17,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	5,7,10,18	2,4,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	5,7,10,16,17	2,4,8,9,13,15,17	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	5,7,10,14,17,18	2,4,8,9,13,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	5,7,10,14,16	2,4,8,9,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	5,7,10,14,17	2,4,8,9,13,15,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	5,7,10,14,16,18	2,4,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	5,7,10,12,17	2,4,8,9,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	5,7,10,12,16,18	2,4,8,9,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	5,7,10,12,17,18	2,4,8,9,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	5,7,10,12,16	2,4,8,9,15	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	5,7,10,12,14,18	2,4,8,9,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	5,7,10,12,14,16,17	2,4,8,9,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	5,7,10,12,14	2,4,8,9,15	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	5,7,10,12,14,16,17,18	2,4,8,9,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	5,7,10,12,17,18	2,4,8,9,13,17,18	2^{-34}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	5,7,10,12,16	2,4,8,9,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	5,7,10,12,17	2,4,8,9,13,15,17	2^{-34}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	5,7,10,12,16,18	2,4,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	5,7,10,12,14	2,4,8,9,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	5,7,10,12,14,16,17,18	2,4,8,9,13,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	5,7,10,12,14,18	2,4,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	5,7,10,12,14,16,17	2,4,8,9,13,15,17	2^{-23}

Table 0.736 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	5,7,10	2,4,8,9,11	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	5,7,10,16,17,18	2,4,8,9,11,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	5,7,10,18	2,4,8,9,11,15,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	5,7,10,16,17	2,4,8,9,11,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	5,7,10,14,17,18	2,4,8,9,11,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	5,7,10,14,16	2,4,8,9,11	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	5,7,10,14,17	2,4,8,9,11,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	5,7,10,14,16,18	2,4,8,9,11,15,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	5,7,10,18	2,4,8,9,11,13,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	5,7,10,16,17	2,4,8,9,11,13,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	5,7,10	2,4,8,9,11,13,15	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	5,7,10,16,17,18	2,4,8,9,11,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	5,7,10,14,17	2,4,8,9,11,13,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	5,7,10,14,16,18	2,4,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	5,7,10,14,17,18	2,4,8,9,11,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	5,7,10,14,16	2,4,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	5,7,10,12,17,18	2,4,8,9,11,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	5,7,10,12,16	2,4,8,9,11	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	5,7,10,12,17	2,4,8,9,11,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	5,7,10,12,16,18	2,4,8,9,11,15,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	5,7,10,12,14	2,4,8,9,11	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	5,7,10,12,14,16,17,18	2,4,8,9,11,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	5,7,10,12,14,18	2,4,8,9,11,15,18	2^{-12}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	5,7,10,12,14,16,17	2,4,8,9,11,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	5,7,10,12,17	2,4,8,9,11,13,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	5,7,10,12,16,18	2,4,8,9,11,13,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	5,7,10,12,17,18	2,4,8,9,11,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	5,7,10,12,16	2,4,8,9,11,13,15	$2^{-6.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	5,7,10,12,14,18	2,4,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	5,7,10,12,14,16,17	2,4,8,9,11,13,17	2^{-23}
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	5,7,10,12,14	2,4,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	5,7,10,12,14,16,17,18	2,4,8,9,11,13,15,17,18	2^{-23}

Table 0.737 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	5,17	2,4,6,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	5,16,18	2,4,6,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	5,17,18	2,4,6,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	5,16	2,4,6,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	5,14,18	2,4,6,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	5,14,16,17	2,4,6,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	5,14	2,4,6,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	5,14,16,17,18	2,4,6,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	5,17,18	2,4,6,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	5,16	2,4,6,13	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	5,17	2,4,6,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	5,16,18	2,4,6,13,15,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	5,14	2,4,6,13	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	5,14,16,17,18	2,4,6,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	5,14,18	2,4,6,13,15,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	5,14,16,17	2,4,6,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	5,12,18	2,4,6,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	5,12,16,17	2,4,6,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	5,12	2,4,6,15	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	5,12,16,17,18	2,4,6,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	5,12,14,17	2,4,6,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	5,12,14,16,18	2,4,6,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	5,12,14,17,18	2,4,6,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	5,12,14,16	2,4,6,15	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	5,12	2,4,6,13	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	5,12,16,17,18	2,4,6,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	5,12,18	2,4,6,13,15,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	5,12,16,17	2,4,6,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	5,12,14,17,18	2,4,6,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	5,12,14,16	2,4,6,13	2^{-34}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	5,12,14,17	2,4,6,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	5,12,14,16,18	2,4,6,13,15,18	2^{-34}

Table 0.738 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	5,17,18	2,4,6,11,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	5,16	2,4,6,11	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	5,17	2,4,6,11,15,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	5,16,18	2,4,6,11,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	5,14	2,4,6,11	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	5,14,16,17,18	2,4,6,11,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	5,14,18	2,4,6,11,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	5,14,16,17	2,4,6,11,15,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	5,17	2,4,6,11,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	5,16,18	2,4,6,11,13,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	5,17,18	2,4,6,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	5,16	2,4,6,11,13,15	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	5,14,18	2,4,6,11,13,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	5,14,16,17	2,4,6,11,13,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	5,14	2,4,6,11,13,15	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	5,14,16,17,18	2,4,6,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	5,12	2,4,6,11	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	5,12,16,17,18	2,4,6,11,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	5,12,18	2,4,6,11,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	5,12,16,17	2,4,6,11,15,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	5,12,14,17,18	2,4,6,11,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	5,12,14,16	2,4,6,11	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	5,12,14,17	2,4,6,11,15,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	5,12,14,16,18	2,4,6,11,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	5,12,18	2,4,6,11,13,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	5,12,16,17	2,4,6,11,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	5,12	2,4,6,11,13,15	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	5,12,16,17,18	2,4,6,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	5,12,14,17	2,4,6,11,13,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	5,12,14,16,18	2,4,6,11,13,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	5,12,14,17,18	2,4,6,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	5,12,14,16	2,4,6,11,13,15	2^{-23}

Table 0.739 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	5,10,18	2,4,6,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	5,10,16,17	2,4,6,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	5,10	2,4,6,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	5,10,16,17,18	2,4,6,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	5,10,14,17	2,4,6,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	5,10,14,16,18	2,4,6,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	5,10,14,17,18	2,4,6,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	5,10,14,16	2,4,6,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	5,10	2,4,6,13	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	5,10,16,17,18	2,4,6,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	5,10,18	2,4,6,13,15,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	5,10,16,17	2,4,6,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	5,10,14,17,18	2,4,6,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	5,10,14,16	2,4,6,13	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	5,10,14,17	2,4,6,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	5,10,14,16,18	2,4,6,13,15,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	5,10,12,17	2,4,6,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	5,10,12,16,18	2,4,6,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	5,10,12,17,18	2,4,6,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	5,10,12,16	2,4,6,15	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	5,10,12,14,18	2,4,6,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	5,10,12,14,16,17	2,4,6,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	5,10,12,14	2,4,6,15	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	5,10,12,14,16,17,18	2,4,6,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	5,10,12,17,18	2,4,6,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	5,10,12,16	2,4,6,13	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	5,10,12,17	2,4,6,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	5,10,12,16,18	2,4,6,13,15,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	5,10,12,14	2,4,6,13	2^{-1}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	5,10,12,14,16,17,18	2,4,6,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	5,10,12,14,18	2,4,6,13,15,18	2^{-1}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	5,10,12,14,16,17	2,4,6,13,15,17	$2^{-17.5}$

Table 0.740 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	5,10	2,4,6,11	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	5,10,16,17,18	2,4,6,11,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	5,10,18	2,4,6,11,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	5,10,16,17	2,4,6,11,15,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	5,10,14,17,18	2,4,6,11,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	5,10,14,16	2,4,6,11	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	5,10,14,17	2,4,6,11,15,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	5,10,14,16,18	2,4,6,11,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	5,10,18	2,4,6,11,13,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	5,10,16,17	2,4,6,11,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	5,10	2,4,6,11,13,15	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	5,10,16,17,18	2,4,6,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	5,10,14,17	2,4,6,11,13,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	5,10,14,16,18	2,4,6,11,13,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	5,10,14,17,18	2,4,6,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	5,10,14,16	2,4,6,11,13,15	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	5,10,12,17,18	2,4,6,11,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	5,10,12,16	2,4,6,11	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	5,10,12,17	2,4,6,11,15,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	5,10,12,16,18	2,4,6,11,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	5,10,12,14	2,4,6,11	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	5,10,12,14,16,17,18	2,4,6,11,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	5,10,12,14,18	2,4,6,11,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	5,10,12,14,16,17	2,4,6,11,15,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	5,10,12,17	2,4,6,11,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	5,10,12,16,18	2,4,6,11,13,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	5,10,12,17,18	2,4,6,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	5,10,12,16	2,4,6,11,13,15	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	5,10,12,14,18	2,4,6,11,13,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	5,10,12,14,16,17	2,4,6,11,13,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	5,10,12,14	2,4,6,11,13,15	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	5,10,12,14,16,17,18	2,4,6,11,13,15,17,18	$2^{-28.5}$

Table 0.741 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	5,17,18	2,4,6,9,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	5,16	2,4,6,9	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	5,17	2,4,6,9,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	5,16,18	2,4,6,9,15,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	5,14	2,4,6,9	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	5,14,16,17,18	2,4,6,9,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	5,14,18	2,4,6,9,15,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	5,14,16,17	2,4,6,9,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	5,17	2,4,6,9,13,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	5,16,18	2,4,6,9,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	5,17,18	2,4,6,9,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	5,16	2,4,6,9,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	5,14,18	2,4,6,9,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	5,14,16,17	2,4,6,9,13,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	5,14	2,4,6,9,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	5,14,16,17,18	2,4,6,9,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	5,12	2,4,6,9	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	5,12,16,17,18	2,4,6,9,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	5,12,18	2,4,6,9,15,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	5,12,16,17	2,4,6,9,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	5,12,14,17,18	2,4,6,9,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	5,12,14,16	2,4,6,9	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	5,12,14,17	2,4,6,9,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	5,12,14,16,18	2,4,6,9,15,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	5,12,18	2,4,6,9,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	5,12,16,17	2,4,6,9,13,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	5,12	2,4,6,9,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	5,12,16,17,18	2,4,6,9,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	5,12,14,17	2,4,6,9,13,17	2^{-1}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	5,12,14,16,18	2,4,6,9,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	5,12,14,17,18	2,4,6,9,13,15,17,18	2^{-1}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	5,12,14,16	2,4,6,9,13,15	$2^{-17.5}$

Table 0.742 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	5,17	2,4,6,9,11,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	5,16,18	2,4,6,9,11,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	5,17,18	2,4,6,9,11,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	5,16	2,4,6,9,11,15	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	5,14,18	2,4,6,9,11,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	5,14,16,17	2,4,6,9,11,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	5,14	2,4,6,9,11,15	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	5,14,16,17,18	2,4,6,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	5,17,18	2,4,6,9,11,13,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	5,16	2,4,6,9,11,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	5,17	2,4,6,9,11,13,15,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	5,16,18	2,4,6,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	5,14	2,4,6,9,11,13	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	5,14,16,17,18	2,4,6,9,11,13,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	5,14,18	2,4,6,9,11,13,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	5,14,16,17	2,4,6,9,11,13,15,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	5,12,18	2,4,6,9,11,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	5,12,16,17	2,4,6,9,11,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	5,12	2,4,6,9,11,15	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	5,12,16,17,18	2,4,6,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	5,12,14,17	2,4,6,9,11,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	5,12,14,16,18	2,4,6,9,11,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	5,12,14,17,18	2,4,6,9,11,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	5,12,14,16	2,4,6,9,11,15	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	5,12	2,4,6,9,11,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	5,12,16,17,18	2,4,6,9,11,13,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	5,12,18	2,4,6,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	5,12,16,17	2,4,6,9,11,13,15,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	5,12,14,17,18	2,4,6,9,11,13,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	5,12,14,16	2,4,6,9,11,13	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	5,12,14,17	2,4,6,9,11,13,15,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	5,12,14,16,18	2,4,6,9,11,13,15,18	$2^{-28.5}$

Table 0.743 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	5,10	2,4,6,9	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	5,10,16,17,18	2,4,6,9,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	5,10,18	2,4,6,9,15,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	5,10,16,17	2,4,6,9,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	5,10,14,17,18	2,4,6,9,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	5,10,14,16	2,4,6,9	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	5,10,14,17	2,4,6,9,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	5,10,14,16,18	2,4,6,9,15,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	5,10,18	2,4,6,9,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	5,10,16,17	2,4,6,9,13,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	5,10	2,4,6,9,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	5,10,16,17,18	2,4,6,9,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	5,10,14,17	2,4,6,9,13,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	5,10,14,16,18	2,4,6,9,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	5,10,14,17,18	2,4,6,9,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	5,10,14,16	2,4,6,9,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	5,10,12,17,18	2,4,6,9,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	5,10,12,16	2,4,6,9	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	5,10,12,17	2,4,6,9,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	5,10,12,16,18	2,4,6,9,15,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	5,10,12,14	2,4,6,9	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	5,10,12,14,16,17,18	2,4,6,9,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	5,10,12,14,18	2,4,6,9,15,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	5,10,12,14,16,17	2,4,6,9,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	5,10,12,17	2,4,6,9,13,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	5,10,12,16,18	2,4,6,9,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	5,10,12,17,18	2,4,6,9,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	5,10,12,16	2,4,6,9,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	5,10,12,14,18	2,4,6,9,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	5,10,12,14,16,17	2,4,6,9,13,17	2^{-34}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	5,10,12,14	2,4,6,9,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	5,10,12,14,16,17,18	2,4,6,9,13,15,17,18	2^{-34}

Table 0.744 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	5,10,18	2,4,6,9,11,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	5,10,16,17	2,4,6,9,11,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	5,10	2,4,6,9,11,15	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	5,10,16,17,18	2,4,6,9,11,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	5,10,14,17	2,4,6,9,11,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	5,10,14,16,18	2,4,6,9,11,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	5,10,14,17,18	2,4,6,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	5,10,14,16	2,4,6,9,11,15	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	5,10	2,4,6,9,11,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	5,10,16,17,18	2,4,6,9,11,13,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	5,10,18	2,4,6,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	5,10,16,17	2,4,6,9,11,13,15,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	5,10,14,17,18	2,4,6,9,11,13,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	5,10,14,16	2,4,6,9,11,13	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	5,10,14,17	2,4,6,9,11,13,15,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	5,10,14,16,18	2,4,6,9,11,13,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	5,10,12,17	2,4,6,9,11,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	5,10,12,16,18	2,4,6,9,11,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	5,10,12,17,18	2,4,6,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	5,10,12,16	2,4,6,9,11,15	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	5,10,12,14,18	2,4,6,9,11,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	5,10,12,14,16,17	2,4,6,9,11,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	5,10,12,14	2,4,6,9,11,15	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	5,10,12,14,16,17,18	2,4,6,9,11,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	5,10,12,17,18	2,4,6,9,11,13,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	5,10,12,16	2,4,6,9,11,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	5,10,12,17	2,4,6,9,11,13,15,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	5,10,12,16,18	2,4,6,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	5,10,12,14	2,4,6,9,11,13	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	5,10,12,14,16,17,18	2,4,6,9,11,13,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	5,10,12,14,18	2,4,6,9,11,13,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	5,10,12,14,16,17	2,4,6,9,11,13,15,17	2^{-23}

Table 0.745 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	5,18	2,4,6,8,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	5,16,17	2,4,6,8,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	5	2,4,6,8,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	5,16,17,18	2,4,6,8,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	5,14,17	2,4,6,8,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	5,14,16,18	2,4,6,8,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	5,14,17,18	2,4,6,8,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	5,14,16	2,4,6,8,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	5	2,4,6,8,13	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	5,16,17,18	2,4,6,8,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	5,18	2,4,6,8,13,15,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	5,16,17	2,4,6,8,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	5,14,17,18	2,4,6,8,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	5,14,16	2,4,6,8,13	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	5,14,17	2,4,6,8,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	5,14,16,18	2,4,6,8,13,15,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	5,12,17	2,4,6,8,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	5,12,16,18	2,4,6,8,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	5,12,17,18	2,4,6,8,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	5,12,16	2,4,6,8,15	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	5,12,14,18	2,4,6,8,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	5,12,14,16,17	2,4,6,8,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	5,12,14	2,4,6,8,15	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	5,12,14,16,17,18	2,4,6,8,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	5,12,17,18	2,4,6,8,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	5,12,16	2,4,6,8,13	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	5,12,17	2,4,6,8,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	5,12,16,18	2,4,6,8,13,15,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	5,12,14	2,4,6,8,13	2^{-34}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	5,12,14,16,17,18	2,4,6,8,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	5,12,14,18	2,4,6,8,13,15,18	2^{-34}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	5,12,14,16,17	2,4,6,8,13,15,17	$2^{-17.5}$

Table 0.746 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	5	2,4,6,8,11	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	5,16,17,18	2,4,6,8,11,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	5,18	2,4,6,8,11,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	5,16,17	2,4,6,8,11,15,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	5,14,17,18	2,4,6,8,11,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	5,14,16	2,4,6,8,11	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	5,14,17	2,4,6,8,11,15,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	5,14,16,18	2,4,6,8,11,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	5,18	2,4,6,8,11,13,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	5,16,17	2,4,6,8,11,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	5	2,4,6,8,11,13,15	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	5,16,17,18	2,4,6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	5,14,17	2,4,6,8,11,13,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	5,14,16,18	2,4,6,8,11,13,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	5,14,17,18	2,4,6,8,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	5,14,16	2,4,6,8,11,13,15	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	5,12,17,18	2,4,6,8,11,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	5,12,16	2,4,6,8,11	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	5,12,17	2,4,6,8,11,15,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	5,12,16,18	2,4,6,8,11,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	5,12,14	2,4,6,8,11	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	5,12,14,16,17,18	2,4,6,8,11,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	5,12,14,18	2,4,6,8,11,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	5,12,14,16,17	2,4,6,8,11,15,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	5,12,17	2,4,6,8,11,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	5,12,16,18	2,4,6,8,11,13,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	5,12,17,18	2,4,6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	5,12,16	2,4,6,8,11,13,15	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	5,12,14,18	2,4,6,8,11,13,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	5,12,14,16,17	2,4,6,8,11,13,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	5,12,14	2,4,6,8,11,13,15	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	5,12,14,16,17,18	2,4,6,8,11,13,15,17,18	$2^{-6.5}$

Table 0.747 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	5,10,17	2,4,6,8,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	5,10,16,18	2,4,6,8,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	5,10,17,18	2,4,6,8,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	5,10,16	2,4,6,8,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	5,10,14,18	2,4,6,8,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	5,10,14,16,17	2,4,6,8,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	5,10,14	2,4,6,8,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	5,10,14,16,17,18	2,4,6,8,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	5,10,17,18	2,4,6,8,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	5,10,16	2,4,6,8,13	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	5,10,17	2,4,6,8,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	5,10,16,18	2,4,6,8,13,15,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	5,10,14	2,4,6,8,13	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	5,10,14,16,17,18	2,4,6,8,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	5,10,14,18	2,4,6,8,13,15,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	5,10,14,16,17	2,4,6,8,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	5,10,12,18	2,4,6,8,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	5,10,12,16,17	2,4,6,8,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	5,10,12	2,4,6,8,15	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	5,10,12,16,17,18	2,4,6,8,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	5,10,12,14,17	2,4,6,8,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	5,10,12,14,16,18	2,4,6,8,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	5,10,12,14,17,18	2,4,6,8,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	5,10,12,14,16	2,4,6,8,15	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	5,10,12	2,4,6,8,13	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	5,10,12,16,17,18	2,4,6,8,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	5,10,12,18	2,4,6,8,13,15,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	5,10,12,16,17	2,4,6,8,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	5,10,12,14,17,18	2,4,6,8,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	5,10,12,14,16	2,4,6,8,13	2^{-1}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	5,10,12,14,17	2,4,6,8,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	5,10,12,14,16,18	2,4,6,8,13,15,18	2^{-1}

Table 0.748 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	5,10,17,18	2,4,6,8,11,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	5,10,16	2,4,6,8,11	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	5,10,17	2,4,6,8,11,15,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	5,10,16,18	2,4,6,8,11,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	5,10,14	2,4,6,8,11	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	5,10,14,16,17,18	2,4,6,8,11,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	5,10,14,18	2,4,6,8,11,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	5,10,14,16,17	2,4,6,8,11,15,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	5,10,17	2,4,6,8,11,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	5,10,16,18	2,4,6,8,11,13,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	5,10,17,18	2,4,6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	5,10,16	2,4,6,8,11,13,15	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	5,10,14,18	2,4,6,8,11,13,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	5,10,14,16,17	2,4,6,8,11,13,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	5,10,14	2,4,6,8,11,13,15	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	5,10,14,16,17,18	2,4,6,8,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	5,10,12	2,4,6,8,11	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	5,10,12,16,17,18	2,4,6,8,11,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	5,10,12,18	2,4,6,8,11,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	5,10,12,16,17	2,4,6,8,11,15,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	5,10,12,14,17,18	2,4,6,8,11,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	5,10,12,14,16	2,4,6,8,11	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	5,10,12,14,17	2,4,6,8,11,15,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	5,10,12,14,16,18	2,4,6,8,11,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	5,10,12,18	2,4,6,8,11,13,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	5,10,12,16,17	2,4,6,8,11,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	5,10,12	2,4,6,8,11,13,15	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	5,10,12,16,17,18	2,4,6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	5,10,12,14,17	2,4,6,8,11,13,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	5,10,12,14,16,18	2,4,6,8,11,13,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	5,10,12,14,17,18	2,4,6,8,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	5,10,12,14,16	2,4,6,8,11,13,15	2^{-12}

Table 0.749 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	5	2,4,6,8,9	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	5,16,17,18	2,4,6,8,9,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	5,18	2,4,6,8,9,15,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	5,16,17	2,4,6,8,9,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	5,14,17,18	2,4,6,8,9,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	5,14,16	2,4,6,8,9	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	5,14,17	2,4,6,8,9,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	5,14,16,18	2,4,6,8,9,15,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	5,18	2,4,6,8,9,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	5,16,17	2,4,6,8,9,13,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	5	2,4,6,8,9,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	5,16,17,18	2,4,6,8,9,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	5,14,17	2,4,6,8,9,13,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	5,14,16,18	2,4,6,8,9,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	5,14,17,18	2,4,6,8,9,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	5,14,16	2,4,6,8,9,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	5,12,17,18	2,4,6,8,9,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	5,12,16	2,4,6,8,9	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	5,12,17	2,4,6,8,9,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	5,12,16,18	2,4,6,8,9,15,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	5,12,14	2,4,6,8,9	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	5,12,14,16,17,18	2,4,6,8,9,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	5,12,14,18	2,4,6,8,9,15,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	5,12,14,16,17	2,4,6,8,9,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	5,12,17	2,4,6,8,9,13,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	5,12,16,18	2,4,6,8,9,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	5,12,17,18	2,4,6,8,9,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	5,12,16	2,4,6,8,9,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	5,12,14,18	2,4,6,8,9,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	5,12,14,16,17	2,4,6,8,9,13,17	2^{-1}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	5,12,14	2,4,6,8,9,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	5,12,14,16,17,18	2,4,6,8,9,13,15,17,18	2^{-1}

Table 0.750 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	5,18	2,4,6,8,9,11,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	5,16,17	2,4,6,8,9,11,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	5	2,4,6,8,9,11,15	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	5,16,17,18	2,4,6,8,9,11,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	5,14,17	2,4,6,8,9,11,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	5,14,16,18	2,4,6,8,9,11,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	5,14,17,18	2,4,6,8,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	5,14,16	2,4,6,8,9,11,15	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	5	2,4,6,8,9,11,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	5,16,17,18	2,4,6,8,9,11,13,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	5,18	2,4,6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	5,16,17	2,4,6,8,9,11,13,15,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	5,14,17,18	2,4,6,8,9,11,13,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	5,14,16	2,4,6,8,9,11,13	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	5,14,17	2,4,6,8,9,11,13,15,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	5,14,16,18	2,4,6,8,9,11,13,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	5,12,17	2,4,6,8,9,11,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	5,12,16,18	2,4,6,8,9,11,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	5,12,17,18	2,4,6,8,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	5,12,16	2,4,6,8,9,11,15	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	5,12,14,18	2,4,6,8,9,11,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	5,12,14,16,17	2,4,6,8,9,11,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	5,12,14	2,4,6,8,9,11,15	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	5,12,14,16,17,18	2,4,6,8,9,11,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	5,12,17,18	2,4,6,8,9,11,13,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	5,12,16	2,4,6,8,9,11,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	5,12,17	2,4,6,8,9,11,13,15,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	5,12,16,18	2,4,6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	5,12,14	2,4,6,8,9,11,13	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	5,12,14,16,17,18	2,4,6,8,9,11,13,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	5,12,14,18	2,4,6,8,9,11,13,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	5,12,14,16,17	2,4,6,8,9,11,13,15,17	2^{-12}

Table 0.751 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	5,10,17,18	2,4,6,8,9,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	5,10,16	2,4,6,8,9	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	5,10,17	2,4,6,8,9,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	5,10,16,18	2,4,6,8,9,15,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	5,10,14	2,4,6,8,9	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	5,10,14,16,17,18	2,4,6,8,9,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	5,10,14,18	2,4,6,8,9,15,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	5,10,14,16,17	2,4,6,8,9,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	5,10,17	2,4,6,8,9,13,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	5,10,16,18	2,4,6,8,9,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	5,10,17,18	2,4,6,8,9,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	5,10,16	2,4,6,8,9,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	5,10,14,18	2,4,6,8,9,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	5,10,14,16,17	2,4,6,8,9,13,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	5,10,14	2,4,6,8,9,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	5,10,14,16,17,18	2,4,6,8,9,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	5,10,12	2,4,6,8,9	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	5,10,12,16,17,18	2,4,6,8,9,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	5,10,12,18	2,4,6,8,9,15,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	5,10,12,16,17	2,4,6,8,9,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	5,10,12,14,17,18	2,4,6,8,9,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	5,10,12,14,16	2,4,6,8,9	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	5,10,12,14,17	2,4,6,8,9,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	5,10,12,14,16,18	2,4,6,8,9,15,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	5,10,12,18	2,4,6,8,9,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	5,10,12,16,17	2,4,6,8,9,13,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	5,10,12	2,4,6,8,9,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	5,10,12,16,17,18	2,4,6,8,9,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	5,10,12,14,17	2,4,6,8,9,13,17	2^{-34}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	5,10,12,14,16,18	2,4,6,8,9,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	5,10,12,14,17,18	2,4,6,8,9,13,15,17,18	2^{-34}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	5,10,12,14,16	2,4,6,8,9,13,15	$2^{-17.5}$

Table 0.752 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	5,10,17	2,4,6,8,9,11,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	5,10,16,18	2,4,6,8,9,11,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	5,10,17,18	2,4,6,8,9,11,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	5,10,16	2,4,6,8,9,11,15	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	5,10,14,18	2,4,6,8,9,11,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	5,10,14,16,17	2,4,6,8,9,11,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	5,10,14	2,4,6,8,9,11,15	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	5,10,14,16,17,18	2,4,6,8,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	5,10,17,18	2,4,6,8,9,11,13,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	5,10,16	2,4,6,8,9,11,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	5,10,17	2,4,6,8,9,11,13,15,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	5,10,16,18	2,4,6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	5,10,14	2,4,6,8,9,11,13	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	5,10,14,16,17,18	2,4,6,8,9,11,13,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	5,10,14,18	2,4,6,8,9,11,13,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	5,10,14,16,17	2,4,6,8,9,11,13,15,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	5,10,12,18	2,4,6,8,9,11,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	5,10,12,16,17	2,4,6,8,9,11,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	5,10,12	2,4,6,8,9,11,15	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	5,10,12,16,17,18	2,4,6,8,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	5,10,12,14,17	2,4,6,8,9,11,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	5,10,12,14,16,18	2,4,6,8,9,11,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	5,10,12,14,17,18	2,4,6,8,9,11,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	5,10,12,14,16	2,4,6,8,9,11,15	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	5,10,12	2,4,6,8,9,11,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	5,10,12,16,17,18	2,4,6,8,9,11,13,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	5,10,12,18	2,4,6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	5,10,12,16,17	2,4,6,8,9,11,13,15,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	5,10,12,14,17,18	2,4,6,8,9,11,13,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	5,10,12,14,16	2,4,6,8,9,11,13	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	5,10,12,14,17	2,4,6,8,9,11,13,15,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	5,10,12,14,16,18	2,4,6,8,9,11,13,15,18	$2^{-6.5}$

Table 0.753 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	5,7,17,18	2,4,6,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	5,7,16	2,4,6	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	5,7,17	2,4,6,15,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	5,7,16,18	2,4,6,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	5,7,14	2,4,6	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	5,7,14,16,17,18	2,4,6,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	5,7,14,18	2,4,6,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	5,7,14,16,17	2,4,6,15,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	5,7,17	2,4,6,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	5,7,16,18	2,4,6,13,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	5,7,17,18	2,4,6,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	5,7,16	2,4,6,13,15	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	5,7,14,18	2,4,6,13,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	5,7,14,16,17	2,4,6,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	5,7,14	2,4,6,13,15	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	5,7,14,16,17,18	2,4,6,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	5,7,12	2,4,6	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	5,7,12,16,17,18	2,4,6,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	5,7,12,18	2,4,6,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	5,7,12,16,17	2,4,6,15,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	5,7,12,14,17,18	2,4,6,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	5,7,12,14,16	2,4,6	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	5,7,12,14,17	2,4,6,15,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	5,7,12,14,16,18	2,4,6,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	5,7,12,18	2,4,6,13,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	5,7,12,16,17	2,4,6,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	5,7,12	2,4,6,13,15	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	5,7,12,16,17,18	2,4,6,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	5,7,12,14,17	2,4,6,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	5,7,12,14,16,18	2,4,6,13,18	2^{-34}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	5,7,12,14,17,18	2,4,6,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	5,7,12,14,16	2,4,6,13,15	2^{-34}

Table 0.754 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	5,7,17	2,4,6,11,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	5,7,16,18	2,4,6,11,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	5,7,17,18	2,4,6,11,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	5,7,16	2,4,6,11,15	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	5,7,14,18	2,4,6,11,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	5,7,14,16,17	2,4,6,11,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	5,7,14	2,4,6,11,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	5,7,14,16,17,18	2,4,6,11,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	5,7,17,18	2,4,6,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	5,7,16	2,4,6,11,13	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	5,7,17	2,4,6,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	5,7,16,18	2,4,6,11,13,15,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	5,7,14	2,4,6,11,13	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	5,7,14,16,17,18	2,4,6,11,13,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	5,7,14,18	2,4,6,11,13,15,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	5,7,14,16,17	2,4,6,11,13,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	5,7,12,18	2,4,6,11,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	5,7,12,16,17	2,4,6,11,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	5,7,12	2,4,6,11,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	5,7,12,16,17,18	2,4,6,11,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	5,7,12,14,17	2,4,6,11,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	5,7,12,14,16,18	2,4,6,11,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	5,7,12,14,17,18	2,4,6,11,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	5,7,12,14,16	2,4,6,11,15	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	5,7,12	2,4,6,11,13	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	5,7,12,16,17,18	2,4,6,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	5,7,12,18	2,4,6,11,13,15,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	5,7,12,16,17	2,4,6,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	5,7,12,14,17,18	2,4,6,11,13,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	5,7,12,14,16	2,4,6,11,13	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	5,7,12,14,17	2,4,6,11,13,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	5,7,12,14,16,18	2,4,6,11,13,15,18	2^{-23}

Table 0.755 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	5,7,10	2,4,6	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	5,7,10,16,17,18	2,4,6,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	5,7,10,18	2,4,6,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	5,7,10,16,17	2,4,6,15,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	5,7,10,14,17,18	2,4,6,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	5,7,10,14,16	2,4,6	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	5,7,10,14,17	2,4,6,15,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	5,7,10,14,16,18	2,4,6,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	5,7,10,18	2,4,6,13,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	5,7,10,16,17	2,4,6,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	5,7,10	2,4,6,13,15	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	5,7,10,16,17,18	2,4,6,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	5,7,10,14,17	2,4,6,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	5,7,10,14,16,18	2,4,6,13,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	5,7,10,14,17,18	2,4,6,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	5,7,10,14,16	2,4,6,13,15	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	5,7,10,12,17,18	2,4,6,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	5,7,10,12,16	2,4,6	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	5,7,10,12,17	2,4,6,15,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	5,7,10,12,16,18	2,4,6,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	5,7,10,12,14	2,4,6	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	5,7,10,12,14,16,17,18	2,4,6,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	5,7,10,12,14,18	2,4,6,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	5,7,10,12,14,16,17	2,4,6,15,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	5,7,10,12,17	2,4,6,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	5,7,10,12,16,18	2,4,6,13,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	5,7,10,12,17,18	2,4,6,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	5,7,10,12,16	2,4,6,13,15	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	5,7,10,12,14,18	2,4,6,13,18	2^{-1}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	5,7,10,12,14,16,17	2,4,6,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	5,7,10,12,14	2,4,6,13,15	2^{-1}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	5,7,10,12,14,16,17,18	2,4,6,13,15,17,18	$2^{-17.5}$

Table 0.756 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	5,7,10,18	2,4,6,11,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	5,7,10,16,17	2,4,6,11,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	5,7,10	2,4,6,11,15	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	5,7,10,16,17,18	2,4,6,11,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	5,7,10,14,17	2,4,6,11,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	5,7,10,14,16,18	2,4,6,11,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	5,7,10,14,17,18	2,4,6,11,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	5,7,10,14,16	2,4,6,11,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	5,7,10	2,4,6,11,13	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	5,7,10,16,17,18	2,4,6,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	5,7,10,18	2,4,6,11,13,15,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	5,7,10,16,17	2,4,6,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	5,7,10,14,17,18	2,4,6,11,13,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	5,7,10,14,16	2,4,6,11,13	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	5,7,10,14,17	2,4,6,11,13,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	5,7,10,14,16,18	2,4,6,11,13,15,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	5,7,10,12,17	2,4,6,11,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	5,7,10,12,16,18	2,4,6,11,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	5,7,10,12,17,18	2,4,6,11,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	5,7,10,12,16	2,4,6,11,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	5,7,10,12,14,18	2,4,6,11,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	5,7,10,12,14,16,17	2,4,6,11,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	5,7,10,12,14	2,4,6,11,15	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	5,7,10,12,14,16,17,18	2,4,6,11,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	5,7,10,12,17,18	2,4,6,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	5,7,10,12,16	2,4,6,11,13	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	5,7,10,12,17	2,4,6,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	5,7,10,12,16,18	2,4,6,11,13,15,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	5,7,10,12,14	2,4,6,11,13	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	5,7,10,12,14,16,17,18	2,4,6,11,13,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	5,7,10,12,14,18	2,4,6,11,13,15,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	5,7,10,12,14,16,17	2,4,6,11,13,15,17	$2^{-28.5}$

Table 0.757 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	5,7,17	2,4,6,9,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	5,7,16,18	2,4,6,9,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	5,7,17,18	2,4,6,9,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	5,7,16	2,4,6,9,15	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	5,7,14,18	2,4,6,9,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	5,7,14,16,17	2,4,6,9,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	5,7,14	2,4,6,9,15	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	5,7,14,16,17,18	2,4,6,9,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	5,7,17,18	2,4,6,9,13,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	5,7,16	2,4,6,9,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	5,7,17	2,4,6,9,13,15,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	5,7,16,18	2,4,6,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	5,7,14	2,4,6,9,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	5,7,14,16,17,18	2,4,6,9,13,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	5,7,14,18	2,4,6,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	5,7,14,16,17	2,4,6,9,13,15,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	5,7,12,18	2,4,6,9,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	5,7,12,16,17	2,4,6,9,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	5,7,12	2,4,6,9,15	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	5,7,12,16,17,18	2,4,6,9,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	5,7,12,14,17	2,4,6,9,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	5,7,12,14,16,18	2,4,6,9,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	5,7,12,14,17,18	2,4,6,9,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	5,7,12,14,16	2,4,6,9,15	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	5,7,12	2,4,6,9,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	5,7,12,16,17,18	2,4,6,9,13,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	5,7,12,18	2,4,6,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	5,7,12,16,17	2,4,6,9,13,15,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	5,7,12,14,17,18	2,4,6,9,13,17,18	2^{-1}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	5,7,12,14,16	2,4,6,9,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	5,7,12,14,17	2,4,6,9,13,15,17	2^{-1}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	5,7,12,14,16,18	2,4,6,9,13,15,18	$2^{-17.5}$

Table 0.758 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	5,7,17,18	2,4,6,9,11,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	5,7,16	2,4,6,9,11	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	5,7,17	2,4,6,9,11,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	5,7,16,18	2,4,6,9,11,15,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	5,7,14	2,4,6,9,11	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	5,7,14,16,17,18	2,4,6,9,11,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	5,7,14,18	2,4,6,9,11,15,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	5,7,14,16,17	2,4,6,9,11,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	5,7,17	2,4,6,9,11,13,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	5,7,16,18	2,4,6,9,11,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	5,7,17,18	2,4,6,9,11,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	5,7,16	2,4,6,9,11,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	5,7,14,18	2,4,6,9,11,13,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	5,7,14,16,17	2,4,6,9,11,13,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	5,7,14	2,4,6,9,11,13,15	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	5,7,14,16,17,18	2,4,6,9,11,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	5,7,12	2,4,6,9,11	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	5,7,12,16,17,18	2,4,6,9,11,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	5,7,12,18	2,4,6,9,11,15,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	5,7,12,16,17	2,4,6,9,11,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	5,7,12,14,17,18	2,4,6,9,11,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	5,7,12,14,16	2,4,6,9,11	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	5,7,12,14,17	2,4,6,9,11,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	5,7,12,14,16,18	2,4,6,9,11,15,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	5,7,12,18	2,4,6,9,11,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	5,7,12,16,17	2,4,6,9,11,13,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	5,7,12	2,4,6,9,11,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	5,7,12,16,17,18	2,4,6,9,11,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	5,7,12,14,17	2,4,6,9,11,13,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	5,7,12,14,16,18	2,4,6,9,11,13,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	5,7,12,14,17,18	2,4,6,9,11,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	5,7,12,14,16	2,4,6,9,11,13,15	$2^{-28.5}$

Table 0.759 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	5,7,10,18	2,4,6,9,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	5,7,10,16,17	2,4,6,9,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	5,7,10	2,4,6,9,15	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	5,7,10,16,17,18	2,4,6,9,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	5,7,10,14,17	2,4,6,9,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	5,7,10,14,16,18	2,4,6,9,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	5,7,10,14,17,18	2,4,6,9,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	5,7,10,14,16	2,4,6,9,15	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	5,7,10	2,4,6,9,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	5,7,10,16,17,18	2,4,6,9,13,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	5,7,10,18	2,4,6,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	5,7,10,16,17	2,4,6,9,13,15,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	5,7,10,14,17,18	2,4,6,9,13,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	5,7,10,14,16	2,4,6,9,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	5,7,10,14,17	2,4,6,9,13,15,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	5,7,10,14,16,18	2,4,6,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	5,7,10,12,17	2,4,6,9,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	5,7,10,12,16,18	2,4,6,9,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	5,7,10,12,17,18	2,4,6,9,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	5,7,10,12,16	2,4,6,9,15	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	5,7,10,12,14,18	2,4,6,9,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	5,7,10,12,14,16,17	2,4,6,9,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	5,7,10,12,14	2,4,6,9,15	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	5,7,10,12,14,16,17,18	2,4,6,9,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	5,7,10,12,17,18	2,4,6,9,13,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	5,7,10,12,16	2,4,6,9,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	5,7,10,12,17	2,4,6,9,13,15,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	5,7,10,12,16,18	2,4,6,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	5,7,10,12,14	2,4,6,9,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	5,7,10,12,14,16,17,18	2,4,6,9,13,17,18	2^{-34}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	5,7,10,12,14,18	2,4,6,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	5,7,10,12,14,16,17	2,4,6,9,13,15,17	2^{-34}

Table 0.760 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	5,7,10	2,4,6,9,11	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	5,7,10,16,17,18	2,4,6,9,11,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	5,7,10,18	2,4,6,9,11,15,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	5,7,10,16,17	2,4,6,9,11,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	5,7,10,14,17,18	2,4,6,9,11,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	5,7,10,14,16	2,4,6,9,11	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	5,7,10,14,17	2,4,6,9,11,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	5,7,10,14,16,18	2,4,6,9,11,15,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	5,7,10,18	2,4,6,9,11,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	5,7,10,16,17	2,4,6,9,11,13,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	5,7,10	2,4,6,9,11,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	5,7,10,16,17,18	2,4,6,9,11,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	5,7,10,14,17	2,4,6,9,11,13,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	5,7,10,14,16,18	2,4,6,9,11,13,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	5,7,10,14,17,18	2,4,6,9,11,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	5,7,10,14,16	2,4,6,9,11,13,15	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	5,7,10,12,17,18	2,4,6,9,11,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	5,7,10,12,16	2,4,6,9,11	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	5,7,10,12,17	2,4,6,9,11,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	5,7,10,12,16,18	2,4,6,9,11,15,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	5,7,10,12,14	2,4,6,9,11	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	5,7,10,12,14,16,17,18	2,4,6,9,11,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	5,7,10,12,14,18	2,4,6,9,11,15,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	5,7,10,12,14,16,17	2,4,6,9,11,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	5,7,10,12,17	2,4,6,9,11,13,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	5,7,10,12,16,18	2,4,6,9,11,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	5,7,10,12,17,18	2,4,6,9,11,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	5,7,10,12,16	2,4,6,9,11,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	5,7,10,12,14,18	2,4,6,9,11,13,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	5,7,10,12,14,16,17	2,4,6,9,11,13,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	5,7,10,12,14	2,4,6,9,11,13,15	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	5,7,10,12,14,16,17,18	2,4,6,9,11,13,15,17,18	2^{-23}

Table 0.761 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	5,7	2,4,6,8	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	5,7,16,17,18	2,4,6,8,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	5,7,18	2,4,6,8,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	5,7,16,17	2,4,6,8,15,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	5,7,14,17,18	2,4,6,8,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	5,7,14,16	2,4,6,8	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	5,7,14,17	2,4,6,8,15,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	5,7,14,16,18	2,4,6,8,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	5,7,18	2,4,6,8,13,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	5,7,16,17	2,4,6,8,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	5,7	2,4,6,8,13,15	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	5,7,16,17,18	2,4,6,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	5,7,14,17	2,4,6,8,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	5,7,14,16,18	2,4,6,8,13,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	5,7,14,17,18	2,4,6,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	5,7,14,16	2,4,6,8,13,15	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	5,7,12,17,18	2,4,6,8,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	5,7,12,16	2,4,6,8	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	5,7,12,17	2,4,6,8,15,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	5,7,12,16,18	2,4,6,8,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	5,7,12,14	2,4,6,8	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	5,7,12,14,16,17,18	2,4,6,8,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	5,7,12,14,18	2,4,6,8,15,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	5,7,12,14,16,17	2,4,6,8,15,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	5,7,12,17	2,4,6,8,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	5,7,12,16,18	2,4,6,8,13,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	5,7,12,17,18	2,4,6,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	5,7,12,16	2,4,6,8,13,15	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	5,7,12,14,18	2,4,6,8,13,18	2^{-34}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	5,7,12,14,16,17	2,4,6,8,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	5,7,12,14	2,4,6,8,13,15	2^{-34}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	5,7,12,14,16,17,18	2,4,6,8,13,15,17,18	$2^{-17.5}$

Table 0.762 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	5,7,18	2,4,6,8,11,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	5,7,16,17	2,4,6,8,11,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	5,7	2,4,6,8,11,15	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	5,7,16,17,18	2,4,6,8,11,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	5,7,14,17	2,4,6,8,11,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	5,7,14,16,18	2,4,6,8,11,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	5,7,14,17,18	2,4,6,8,11,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	5,7,14,16	2,4,6,8,11,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	5,7	2,4,6,8,11,13	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	5,7,16,17,18	2,4,6,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	5,7,18	2,4,6,8,11,13,15,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	5,7,16,17	2,4,6,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	5,7,14,17,18	2,4,6,8,11,13,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	5,7,14,16	2,4,6,8,11,13	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	5,7,14,17	2,4,6,8,11,13,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	5,7,14,16,18	2,4,6,8,11,13,15,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	5,7,12,17	2,4,6,8,11,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	5,7,12,16,18	2,4,6,8,11,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	5,7,12,17,18	2,4,6,8,11,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	5,7,12,16	2,4,6,8,11,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	5,7,12,14,18	2,4,6,8,11,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	5,7,12,14,16,17	2,4,6,8,11,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	5,7,12,14	2,4,6,8,11,15	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	5,7,12,14,16,17,18	2,4,6,8,11,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	5,7,12,17,18	2,4,6,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	5,7,12,16	2,4,6,8,11,13	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	5,7,12,17	2,4,6,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	5,7,12,16,18	2,4,6,8,11,13,15,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	5,7,12,14	2,4,6,8,11,13	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	5,7,12,14,16,17,18	2,4,6,8,11,13,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	5,7,12,14,18	2,4,6,8,11,13,15,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	5,7,12,14,16,17	2,4,6,8,11,13,15,17	$2^{-6.5}$

Table 0.763 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	5,7,10,17,18	2,4,6,8,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	5,7,10,16	2,4,6,8	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	5,7,10,17	2,4,6,8,15,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	5,7,10,16,18	2,4,6,8,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	5,7,10,14	2,4,6,8	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	5,7,10,14,16,17,18	2,4,6,8,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	5,7,10,14,18	2,4,6,8,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	5,7,10,14,16,17	2,4,6,8,15,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	5,7,10,17	2,4,6,8,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	5,7,10,16,18	2,4,6,8,13,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	5,7,10,17,18	2,4,6,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	5,7,10,16	2,4,6,8,13,15	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	5,7,10,14,18	2,4,6,8,13,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	5,7,10,14,16,17	2,4,6,8,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	5,7,10,14	2,4,6,8,13,15	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	5,7,10,14,16,17,18	2,4,6,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	5,7,10,12	2,4,6,8	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	5,7,10,12,16,17,18	2,4,6,8,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	5,7,10,12,18	2,4,6,8,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	5,7,10,12,16,17	2,4,6,8,15,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	5,7,10,12,14,17,18	2,4,6,8,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	5,7,10,12,14,16	2,4,6,8	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	5,7,10,12,14,17	2,4,6,8,15,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	5,7,10,12,14,16,18	2,4,6,8,15,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	5,7,10,12,18	2,4,6,8,13,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	5,7,10,12,16,17	2,4,6,8,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	5,7,10,12	2,4,6,8,13,15	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	5,7,10,12,16,17,18	2,4,6,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	5,7,10,12,14,17	2,4,6,8,13,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	5,7,10,12,14,16,18	2,4,6,8,13,18	2^{-1}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	5,7,10,12,14,17,18	2,4,6,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	5,7,10,12,14,16	2,4,6,8,13,15	2^{-1}

Table 0.764 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	5,7,10,17	2,4,6,8,11,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	5,7,10,16,18	2,4,6,8,11,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	5,7,10,17,18	2,4,6,8,11,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	5,7,10,16	2,4,6,8,11,15	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	5,7,10,14,18	2,4,6,8,11,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	5,7,10,14,16,17	2,4,6,8,11,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	5,7,10,14	2,4,6,8,11,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	5,7,10,14,16,17,18	2,4,6,8,11,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	5,7,10,17,18	2,4,6,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	5,7,10,16	2,4,6,8,11,13	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	5,7,10,17	2,4,6,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	5,7,10,16,18	2,4,6,8,11,13,15,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	5,7,10,14	2,4,6,8,11,13	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	5,7,10,14,16,17,18	2,4,6,8,11,13,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	5,7,10,14,18	2,4,6,8,11,13,15,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	5,7,10,14,16,17	2,4,6,8,11,13,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	5,7,10,12,18	2,4,6,8,11,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	5,7,10,12,16,17	2,4,6,8,11,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	5,7,10,12	2,4,6,8,11,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	5,7,10,12,16,17,18	2,4,6,8,11,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	5,7,10,12,14,17	2,4,6,8,11,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	5,7,10,12,14,16,18	2,4,6,8,11,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	5,7,10,12,14,17,18	2,4,6,8,11,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	5,7,10,12,14,16	2,4,6,8,11,15	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	5,7,10,12	2,4,6,8,11,13	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	5,7,10,12,16,17,18	2,4,6,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	5,7,10,12,18	2,4,6,8,11,13,15,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	5,7,10,12,16,17	2,4,6,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	5,7,10,12,14,17,18	2,4,6,8,11,13,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	5,7,10,12,14,16	2,4,6,8,11,13	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	5,7,10,12,14,17	2,4,6,8,11,13,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	5,7,10,12,14,16,18	2,4,6,8,11,13,15,18	2^{-12}

Table 0.765 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	5,7,18	2,4,6,8,9,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	5,7,16,17	2,4,6,8,9,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	5,7	2,4,6,8,9,15	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	5,7,16,17,18	2,4,6,8,9,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	5,7,14,17	2,4,6,8,9,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	5,7,14,16,18	2,4,6,8,9,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	5,7,14,17,18	2,4,6,8,9,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	5,7,14,16	2,4,6,8,9,15	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	5,7	2,4,6,8,9,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	5,7,16,17,18	2,4,6,8,9,13,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	5,7,18	2,4,6,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	5,7,16,17	2,4,6,8,9,13,15,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	5,7,14,17,18	2,4,6,8,9,13,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	5,7,14,16	2,4,6,8,9,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	5,7,14,17	2,4,6,8,9,13,15,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	5,7,14,16,18	2,4,6,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	5,7,12,17	2,4,6,8,9,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	5,7,12,16,18	2,4,6,8,9,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	5,7,12,17,18	2,4,6,8,9,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	5,7,12,16	2,4,6,8,9,15	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	5,7,12,14,18	2,4,6,8,9,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	5,7,12,14,16,17	2,4,6,8,9,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	5,7,12,14	2,4,6,8,9,15	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	5,7,12,14,16,17,18	2,4,6,8,9,15,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	5,7,12,17,18	2,4,6,8,9,13,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	5,7,12,16	2,4,6,8,9,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	5,7,12,17	2,4,6,8,9,13,15,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	5,7,12,16,18	2,4,6,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	5,7,12,14	2,4,6,8,9,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	5,7,12,14,16,17,18	2,4,6,8,9,13,17,18	2^{-1}
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	5,7,12,14,18	2,4,6,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	5,7,12,14,16,17	2,4,6,8,9,13,15,17	2^{-1}

Table 0.766 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	5,7	2,4,6,8,9,11	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	5,7,16,17,18	2,4,6,8,9,11,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	5,7,18	2,4,6,8,9,11,15,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	5,7,16,17	2,4,6,8,9,11,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	5,7,14,17,18	2,4,6,8,9,11,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	5,7,14,16	2,4,6,8,9,11	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	5,7,14,17	2,4,6,8,9,11,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	5,7,14,16,18	2,4,6,8,9,11,15,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	5,7,18	2,4,6,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	5,7,16,17	2,4,6,8,9,11,13,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	5,7	2,4,6,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	5,7,16,17,18	2,4,6,8,9,11,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	5,7,14,17	2,4,6,8,9,11,13,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	5,7,14,16,18	2,4,6,8,9,11,13,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	5,7,14,17,18	2,4,6,8,9,11,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	5,7,14,16	2,4,6,8,9,11,13,15	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	5,7,12,17,18	2,4,6,8,9,11,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	5,7,12,16	2,4,6,8,9,11	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	5,7,12,17	2,4,6,8,9,11,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	5,7,12,16,18	2,4,6,8,9,11,15,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	5,7,12,14	2,4,6,8,9,11	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	5,7,12,14,16,17,18	2,4,6,8,9,11,17,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	5,7,12,14,18	2,4,6,8,9,11,15,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	5,7,12,14,16,17	2,4,6,8,9,11,15,17	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	5,7,12,17	2,4,6,8,9,11,13,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	5,7,12,16,18	2,4,6,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	5,7,12,17,18	2,4,6,8,9,11,13,15,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	5,7,12,16	2,4,6,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	5,7,12,14,18	2,4,6,8,9,11,13,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	5,7,12,14,16,17	2,4,6,8,9,11,13,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	5,7,12,14	2,4,6,8,9,11,13,15	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	5,7,12,14,16,17,18	2,4,6,8,9,11,13,15,17,18	2^{-12}

Table 0.767 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	5,7,10,17	2,4,6,8,9,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	5,7,10,16,18	2,4,6,8,9,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	5,7,10,17,18	2,4,6,8,9,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	5,7,10,16	2,4,6,8,9,15	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	5,7,10,14,18	2,4,6,8,9,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	5,7,10,14,16,17	2,4,6,8,9,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	5,7,10,14	2,4,6,8,9,15	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	5,7,10,14,16,17,18	2,4,6,8,9,15,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	5,7,10,17,18	2,4,6,8,9,13,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	5,7,10,16	2,4,6,8,9,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	5,7,10,17	2,4,6,8,9,13,15,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	5,7,10,16,18	2,4,6,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	5,7,10,14	2,4,6,8,9,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	5,7,10,14,16,17,18	2,4,6,8,9,13,17,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	5,7,10,14,18	2,4,6,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	5,7,10,14,16,17	2,4,6,8,9,13,15,17	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	5,7,10,12,18	2,4,6,8,9,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	5,7,10,12,16,17	2,4,6,8,9,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	5,7,10,12	2,4,6,8,9,15	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	5,7,10,12,16,17,18	2,4,6,8,9,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	5,7,10,12,14,17	2,4,6,8,9,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	5,7,10,12,14,16,18	2,4,6,8,9,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	5,7,10,12,14,17,18	2,4,6,8,9,15,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	5,7,10,12,14,16	2,4,6,8,9,15	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	5,7,10,12	2,4,6,8,9,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	5,7,10,12,16,17,18	2,4,6,8,9,13,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	5,7,10,12,18	2,4,6,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	5,7,10,12,16,17	2,4,6,8,9,13,15,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	5,7,10,12,14,17,18	2,4,6,8,9,13,17,18	2^{-34}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	5,7,10,12,14,16	2,4,6,8,9,13	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	5,7,10,12,14,17	2,4,6,8,9,13,15,17	2^{-34}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	5,7,10,12,14,16,18	2,4,6,8,9,13,15,18	$2^{-17.5}$

Table 0.768 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	5,7,10,17,18	2,4,6,8,9,11,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	5,7,10,16	2,4,6,8,9,11	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	5,7,10,17	2,4,6,8,9,11,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	5,7,10,16,18	2,4,6,8,9,11,15,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	5,7,10,14	2,4,6,8,9,11	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	5,7,10,14,16,17,18	2,4,6,8,9,11,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	5,7,10,14,18	2,4,6,8,9,11,15,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	5,7,10,14,16,17	2,4,6,8,9,11,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	5,7,10,17	2,4,6,8,9,11,13,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	5,7,10,16,18	2,4,6,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	5,7,10,17,18	2,4,6,8,9,11,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	5,7,10,16	2,4,6,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	5,7,10,14,18	2,4,6,8,9,11,13,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	5,7,10,14,16,17	2,4,6,8,9,11,13,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	5,7,10,14	2,4,6,8,9,11,13,15	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	5,7,10,14,16,17,18	2,4,6,8,9,11,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	5,7,10,12	2,4,6,8,9,11	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	5,7,10,12,16,17,18	2,4,6,8,9,11,17,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	5,7,10,12,18	2,4,6,8,9,11,15,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	5,7,10,12,16,17	2,4,6,8,9,11,15,17	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	5,7,10,12,14,17,18	2,4,6,8,9,11,17,18	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	5,7,10,12,14,16	2,4,6,8,9,11	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	5,7,10,12,14,17	2,4,6,8,9,11,15,17	$2^{-28.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	5,7,10,12,14,16,18	2,4,6,8,9,11,15,18	2^{-12}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	5,7,10,12,18	2,4,6,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	5,7,10,12,16,17	2,4,6,8,9,11,13,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	5,7,10,12	2,4,6,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	5,7,10,12,16,17,18	2,4,6,8,9,11,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	5,7,10,12,14,17	2,4,6,8,9,11,13,17	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	5,7,10,12,14,16,18	2,4,6,8,9,11,13,18	$2^{-6.5}$
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	5,7,10,12,14,17,18	2,4,6,8,9,11,13,15,17,18	2^{-23}
$(0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	5,7,10,12,14,16	2,4,6,8,9,11,13,15	$2^{-6.5}$

Table 0.769 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	3,17	2,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	3,16,18	2,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	3,17,18	2,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	3,16	2,15	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	3,14,18	2,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	3,14,16,17	2,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	3,14	2,15	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,14,16,17,18	2,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	3,17,18	2,13,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	3,16	2,13	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	3,17	2,13,15,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	3,16,18	2,13,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	3,14	2,13	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	3,14,16,17,18	2,13,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	3,14,18	2,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,14,16,17	2,13,15,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	3,12,18	2,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	3,12,16,17	2,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	3,12	2,15	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	3,12,16,17,18	2,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,12,14,17	2,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	3,12,14,16,18	2,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	3,12,14,17,18	2,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	3,12,14,16	2,15	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	3,12	2,13	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	3,12,16,17,18	2,13,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	3,12,18	2,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	3,12,16,17	2,13,15,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	3,12,14,17,18	2,13,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	3,12,14,16	2,13	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	3,12,14,17	2,13,15,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	3,12,14,16,18	2,13,15,18	$2^{-28.5}$

Table 0.770 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	3,17,18	2,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	3,16	2,11	2^{-34}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	3,17	2,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	3,16,18	2,11,15,18	2^{-34}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	3,14	2,11	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	3,14,16,17,18	2,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	3,14,18	2,11,15,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	3,14,16,17	2,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	3,17	2,11,13,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	3,16,18	2,11,13,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	3,17,18	2,11,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	3,16	2,11,13,15	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	3,14,18	2,11,13,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	3,14,16,17	2,11,13,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	3,14	2,11,13,15	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	3,14,16,17,18	2,11,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	3,12	2,11	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	3,12,16,17,18	2,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	3,12,18	2,11,15,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	3,12,16,17	2,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	3,12,14,17,18	2,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	3,12,14,16	2,11	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	3,12,14,17	2,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	3,12,14,16,18	2,11,15,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	3,12,18	2,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	3,12,16,17	2,11,13,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	3,12	2,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	3,12,16,17,18	2,11,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	3,12,14,17	2,11,13,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	3,12,14,16,18	2,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	3,12,14,17,18	2,11,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	3,12,14,16	2,11,13,15	$2^{-17.5}$

Table 0.771 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	3,10,18	2,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	3,10,16,17	2,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	3,10	2,15	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	3,10,16,17,18	2,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,10,14,17	2,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	3,10,14,16,18	2,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	3,10,14,17,18	2,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	3,10,14,16	2,15	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	3,10	2,13	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	3,10,16,17,18	2,13,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	3,10,18	2,13,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	3,10,16,17	2,13,15,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	3,10,14,17,18	2,13,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	3,10,14,16	2,13	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	3,10,14,17	2,13,15,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	3,10,14,16,18	2,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	3,10,12,17	2,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	3,10,12,16,18	2,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	3,10,12,17,18	2,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	3,10,12,16	2,15	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	3,10,12,14,18	2,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	3,10,12,14,16,17	2,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	3,10,12,14	2,15	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	3,10,12,14,16,17,18	2,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	3,10,12,17,18	2,13,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	3,10,12,16	2,13	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	3,10,12,17	2,13,15,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	3,10,12,16,18	2,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	3,10,12,14	2,13	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	3,10,12,14,16,17,18	2,13,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	3,10,12,14,18	2,13,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,10,12,14,16,17	2,13,15,17	2^{-12}

Table 0.772 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	3,10	2,11	2^{-1}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	3,10,16,17,18	2,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	3,10,18	2,11,15,18	2^{-1}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	3,10,16,17	2,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	3,10,14,17,18	2,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	3,10,14,16	2,11	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	3,10,14,17	2,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	3,10,14,16,18	2,11,15,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	3,10,18	2,11,13,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	3,10,16,17	2,11,13,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	3,10	2,11,13,15	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	3,10,16,17,18	2,11,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	3,10,14,17	2,11,13,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	3,10,14,16,18	2,11,13,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	3,10,14,17,18	2,11,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	3,10,14,16	2,11,13,15	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	3,10,12,17,18	2,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	3,10,12,16	2,11	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	3,10,12,17	2,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	3,10,12,16,18	2,11,15,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	3,10,12,14	2,11	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	3,10,12,14,16,17,18	2,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,10,12,14,18	2,11,15,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	3,10,12,14,16,17	2,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	3,10,12,17	2,11,13,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	3,10,12,16,18	2,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	3,10,12,17,18	2,11,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	3,10,12,16	2,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	3,10,12,14,18	2,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	3,10,12,14,16,17	2,11,13,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	3,10,12,14	2,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	3,10,12,14,16,17,18	2,11,13,15,17,18	2^{-23}

Table 0.773 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	3,17,18	2,9,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	3,16	2,9	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	3,17	2,9,15,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	3,16,18	2,9,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	3,14	2,9	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	3,14,16,17,18	2,9,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	3,14,18	2,9,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	3,14,16,17	2,9,15,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	3,17	2,9,13,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	3,16,18	2,9,13,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	3,17,18	2,9,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	3,16	2,9,13,15	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	3,14,18	2,9,13,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	3,14,16,17	2,9,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	3,14	2,9,13,15	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	3,14,16,17,18	2,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	3,12	2,9	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	3,12,16,17,18	2,9,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	3,12,18	2,9,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	3,12,16,17	2,9,15,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	3,12,14,17,18	2,9,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	3,12,14,16	2,9	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	3,12,14,17	2,9,15,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	3,12,14,16,18	2,9,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	3,12,18	2,9,13,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	3,12,16,17	2,9,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	3,12	2,9,13,15	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	3,12,16,17,18	2,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	3,12,14,17	2,9,13,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	3,12,14,16,18	2,9,13,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	3,12,14,17,18	2,9,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	3,12,14,16	2,9,13,15	2^{-12}

Table 0.774 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	3,17	2,9,11,17	2^{-1}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	3,16,18	2,9,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	3,17,18	2,9,11,15,17,18	2^{-1}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	3,16	2,9,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	3,14,18	2,9,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	3,14,16,17	2,9,11,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	3,14	2,9,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	3,14,16,17,18	2,9,11,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	3,17,18	2,9,11,13,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	3,16	2,9,11,13	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	3,17	2,9,11,13,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	3,16,18	2,9,11,13,15,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	3,14	2,9,11,13	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	3,14,16,17,18	2,9,11,13,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,14,18	2,9,11,13,15,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	3,14,16,17	2,9,11,13,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	3,12,18	2,9,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	3,12,16,17	2,9,11,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	3,12	2,9,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	3,12,16,17,18	2,9,11,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	3,12,14,17	2,9,11,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	3,12,14,16,18	2,9,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	3,12,14,17,18	2,9,11,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	3,12,14,16	2,9,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	3,12	2,9,11,13	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	3,12,16,17,18	2,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	3,12,18	2,9,11,13,15,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	3,12,16,17	2,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	3,12,14,17,18	2,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	3,12,14,16	2,9,11,13	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	3,12,14,17	2,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	3,12,14,16,18	2,9,11,13,15,18	2^{-23}

Table 0.775 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,10	2,9	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,10,16,17,18	2,9,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	3,10,18	2,9,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	3,10,16,17	2,9,15,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	3,10,14,17,18	2,9,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	3,10,14,16	2,9	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	3,10,14,17	2,9,15,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	3,10,14,16,18	2,9,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	3,10,18	2,9,13,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	3,10,16,17	2,9,13,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	3,10	2,9,13,15	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	3,10,16,17,18	2,9,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	3,10,14,17	2,9,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	3,10,14,16,18	2,9,13,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	3,10,14,17,18	2,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	3,10,14,16	2,9,13,15	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	3,10,12,17,18	2,9,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	3,10,12,16	2,9	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	3,10,12,17	2,9,15,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	3,10,12,16,18	2,9,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	3,10,12,14	2,9	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	3,10,12,14,16,17,18	2,9,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	3,10,12,14,18	2,9,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	3,10,12,14,16,17	2,9,15,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	3,10,12,17,18	2,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	3,10,12,16	2,9,13,15	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	3,10,12,14,18	2,9,13,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	3,10,12,14,16,17	2,9,13,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	3,10,12,14	2,9,13,15	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	3,10,12,14,16,17,18	2,9,13,15,17,18	$2^{-28.5}$

Table 0.776 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	3,10,18	2,9,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	3,10,16,17	2,9,11,17	2^{-34}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	3,10	2,9,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	3,10,16,17,18	2,9,11,15,17,18	2^{-34}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	3,10,14,17	2,9,11,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	3,10,14,16,18	2,9,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,10,14,17,18	2,9,11,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	3,10,14,16	2,9,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	3,10	2,9,11,13	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	3,10,16,17,18	2,9,11,13,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	3,10,18	2,9,11,13,15,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	3,10,16,17	2,9,11,13,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	3,10,14,17,18	2,9,11,13,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	3,10,14,16	2,9,11,13	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,10,14,17	2,9,11,13,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	3,10,14,16,18	2,9,11,13,15,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,10,12,17	2,9,11,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	3,10,12,16,18	2,9,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	3,10,12,17,18	2,9,11,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	3,10,12,16	2,9,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	3,10,12,14,18	2,9,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	3,10,12,14,16,17	2,9,11,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	3,10,12,14	2,9,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	3,10,12,14,16,17,18	2,9,11,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	3,10,12,17,18	2,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	3,10,12,16	2,9,11,13	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	3,10,12,17	2,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	3,10,12,16,18	2,9,11,13,15,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	3,10,12,14	2,9,11,13	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	3,10,12,14,16,17,18	2,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	3,10,12,14,18	2,9,11,13,15,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	3,10,12,14,16,17	2,9,11,13,15,17	$2^{-17.5}$

Table 0.777 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,18	2,8,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,16,17	2,8,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	3	2,8,15	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	3,16,17,18	2,8,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	3,14,17	2,8,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	3,14,16,18	2,8,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	3,14,17,18	2,8,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	3,14,16	2,8,15	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	3	2,8,13	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	3,16,17,18	2,8,13,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	3,18	2,8,13,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	3,16,17	2,8,13,15,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	3,14,17,18	2,8,13,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	3,14,16	2,8,13	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	3,14,17	2,8,13,15,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	3,14,16,18	2,8,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	3,12,17	2,8,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	3,12,16,18	2,8,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	3,12,17,18	2,8,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	3,12,16	2,8,15	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	3,12,14,18	2,8,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	3,12,14,16,17	2,8,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	3,12,14	2,8,15	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	3,12,14,16,17,18	2,8,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	3,12,17,18	2,8,13,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	3,12,16	2,8,13	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	3,12,17	2,8,13,15,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,12,16,18	2,8,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	3,12,14	2,8,13	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	3,12,14,16,17,18	2,8,13,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	3,12,14,18	2,8,13,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	3,12,14,16,17	2,8,13,15,17	2^{-23}

Table 0.778 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	3	2,8,11	2^{-34}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	3,16,17,18	2,8,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	3,18	2,8,11,15,18	2^{-34}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	3,16,17	2,8,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	3,14,17,18	2,8,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	3,14,16	2,8,11	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	3,14,17	2,8,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,14,16,18	2,8,11,15,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	3,18	2,8,11,13,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	3,16,17	2,8,11,13,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	3	2,8,11,13,15	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	3,16,17,18	2,8,11,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	3,14,17	2,8,11,13,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	3,14,16,18	2,8,11,13,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	3,14,17,18	2,8,11,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,14,16	2,8,11,13,15	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	3,12,17,18	2,8,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,12,16	2,8,11	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	3,12,17	2,8,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	3,12,16,18	2,8,11,15,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	3,12,14	2,8,11	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	3,12,14,16,17,18	2,8,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	3,12,14,18	2,8,11,15,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	3,12,14,16,17	2,8,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	3,12,17	2,8,11,13,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	3,12,16,18	2,8,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	3,12,17,18	2,8,11,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	3,12,16	2,8,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	3,12,14,18	2,8,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	3,12,14,16,17	2,8,11,13,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	3,12,14	2,8,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	3,12,14,16,17,18	2,8,11,13,15,17,18	2^{-12}

Table 0.779 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(2)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	3,10,17	2,8,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	3,10,16,18	2,8,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	3,10,17,18	2,8,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	3,10,16	2,8,15	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	3,10,14,18	2,8,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	3,10,14,16,17	2,8,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	3,10,14	2,8,15	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	3,10,14,16,17,18	2,8,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	3,10,17,18	2,8,13,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	3,10,16	2,8,13	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	3,10,17	2,8,13,15,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	3,10,16,18	2,8,13,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	3,10,14	2,8,13	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	3,10,14,16,17,18	2,8,13,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	3,10,14,18	2,8,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	3,10,14,16,17	2,8,13,15,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	3,10,12,18	2,8,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	3,10,12,16,17	2,8,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	3,10,12	2,8,15	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	3,10,12,16,17,18	2,8,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	3,10,12,14,17	2,8,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	3,10,12,14,16,18	2,8,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	3,10,12,14,17,18	2,8,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	3,10,12,14,16	2,8,15	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	3,10,12	2,8,13	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	3,10,12,16,17,18	2,8,13,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	3,10,12,18	2,8,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	3,10,12,16,17	2,8,13,15,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	3,10,12,14,17,18	2,8,13,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	3,10,12,14,16	2,8,13	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	3,10,12,14,17	2,8,13,15,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	3,10,12,14,16,18	2,8,13,15,18	$2^{-6.5}$

Table 0.780 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	3,10,17,18	2,8,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	3,10,16	2,8,11	2^{-1}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	3,10,17	2,8,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	3,10,16,18	2,8,11,15,18	2^{-1}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	3,10,14	2,8,11	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	3,10,14,16,17,18	2,8,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	3,10,14,18	2,8,11,15,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	3,10,14,16,17	2,8,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	3,10,17	2,8,11,13,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	3,10,16,18	2,8,11,13,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	3,10,17,18	2,8,11,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	3,10,16	2,8,11,13,15	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	3,10,14,18	2,8,11,13,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	3,10,14,16,17	2,8,11,13,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	3,10,14	2,8,11,13,15	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,10,14,16,17,18	2,8,11,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	3,10,12	2,8,11	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	3,10,12,16,17,18	2,8,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	3,10,12,18	2,8,11,15,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	3,10,12,16,17	2,8,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	3,10,12,14,17,18	2,8,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	3,10,12,14,16	2,8,11	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	3,10,12,14,17	2,8,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	3,10,12,14,16,18	2,8,11,15,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	3,10,12,18	2,8,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	3,10,12,16,17	2,8,11,13,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	3,10,12	2,8,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	3,10,12,16,17,18	2,8,11,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	3,10,12,14,17	2,8,11,13,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	3,10,12,14,16,18	2,8,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	3,10,12,14,17,18	2,8,11,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	3,10,12,14,16	2,8,11,13,15	$2^{-17.5}$

Table 0.781 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	3	2,8,9	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	3,16,17,18	2,8,9,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	3,18	2,8,9,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	3,16,17	2,8,9,15,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	3,14,17,18	2,8,9,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,14,16	2,8,9	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	3,14,17	2,8,9,15,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	3,14,16,18	2,8,9,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	3,18	2,8,9,13,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	3,16,17	2,8,9,13,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	3	2,8,9,13,15	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	3,16,17,18	2,8,9,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	3,14,17	2,8,9,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	3,14,16,18	2,8,9,13,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	3,14,17,18	2,8,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	3,14,16	2,8,9,13,15	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	3,12,17,18	2,8,9,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	3,12,16	2,8,9	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	3,12,17	2,8,9,15,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	3,12,16,18	2,8,9,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	3,12,14	2,8,9	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	3,12,14,16,17,18	2,8,9,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	3,12,14,18	2,8,9,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	3,12,14,16,17	2,8,9,15,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	3,12,17	2,8,9,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	3,12,16,18	2,8,9,13,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	3,12,17,18	2,8,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	3,12,16	2,8,9,13,15	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	3,12,14,18	2,8,9,13,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	3,12,14,16,17	2,8,9,13,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,12,14	2,8,9,13,15	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	3,12,14,16,17,18	2,8,9,13,15,17,18	$2^{-6.5}$

Table 0.782 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	3,18	2,8,9,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	3,16,17	2,8,9,11,17	2^{-1}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	3	2,8,9,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	3,16,17,18	2,8,9,11,15,17,18	2^{-1}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	3,14,17	2,8,9,11,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	3,14,16,18	2,8,9,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	3,14,17,18	2,8,9,11,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	3,14,16	2,8,9,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	3	2,8,9,11,13	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	3,16,17,18	2,8,9,11,13,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	3,18	2,8,9,11,13,15,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	3,16,17	2,8,9,11,13,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	3,14,17,18	2,8,9,11,13,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	3,14,16	2,8,9,11,13	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	3,14,17	2,8,9,11,13,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	3,14,16,18	2,8,9,11,13,15,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	3,12,17	2,8,9,11,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	3,12,16,18	2,8,9,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	3,12,17,18	2,8,9,11,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	3,12,16	2,8,9,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	3,12,14,18	2,8,9,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	3,12,14,16,17	2,8,9,11,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	3,12,14	2,8,9,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,12,14,16,17,18	2,8,9,11,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	3,12,17,18	2,8,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	3,12,16	2,8,9,11,13	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	3,12,17	2,8,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	3,12,16,18	2,8,9,11,13,15,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	3,12,14	2,8,9,11,13	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	3,12,14,16,17,18	2,8,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	3,12,14,18	2,8,9,11,13,15,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	3,12,14,16,17	2,8,9,11,13,15,17	$2^{-17.5}$

Table 0.783 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	3,10,17,18	2,8,9,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	3,10,16	2,8,9	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	3,10,17	2,8,9,15,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	3,10,16,18	2,8,9,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	3,10,14	2,8,9	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	3,10,14,16,17,18	2,8,9,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,10,14,18	2,8,9,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	3,10,14,16,17	2,8,9,15,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	3,10,17	2,8,9,13,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	3,10,16,18	2,8,9,13,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	3,10,17,18	2,8,9,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	3,10,16	2,8,9,13,15	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	3,10,14,18	2,8,9,13,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	3,10,14,16,17	2,8,9,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,10,14	2,8,9,13,15	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	3,10,14,16,17,18	2,8,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	3,10,12	2,8,9	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	3,10,12,16,17,18	2,8,9,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	3,10,12,18	2,8,9,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	3,10,12,16,17	2,8,9,15,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	3,10,12,14,17,18	2,8,9,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,10,12,14,16	2,8,9	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	3,10,12,14,17	2,8,9,15,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	3,10,12,14,16,18	2,8,9,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	3,10,12,18	2,8,9,13,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	3,10,12,16,17	2,8,9,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	3,10,12	2,8,9,13,15	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	3,10,12,16,17,18	2,8,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	3,10,12,14,17	2,8,9,13,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	3,10,12,14,16,18	2,8,9,13,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	3,10,12,14,17,18	2,8,9,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	3,10,12,14,16	2,8,9,13,15	2^{-23}

Table 0.784 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	3,10,17	2,8,9,11,17	2^{-34}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	3,10,16,18	2,8,9,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	3,10,17,18	2,8,9,11,15,17,18	2^{-34}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	3,10,16	2,8,9,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	3,10,14,18	2,8,9,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	3,10,14,16,17	2,8,9,11,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	3,10,14	2,8,9,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	3,10,14,16,17,18	2,8,9,11,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	3,10,17,18	2,8,9,11,13,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	3,10,16	2,8,9,11,13	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	3,10,17	2,8,9,11,13,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	3,10,16,18	2,8,9,11,13,15,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	3,10,14	2,8,9,11,13	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	3,10,14,16,17,18	2,8,9,11,13,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	3,10,14,18	2,8,9,11,13,15,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	3,10,14,16,17	2,8,9,11,13,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	3,10,12,18	2,8,9,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	3,10,12,16,17	2,8,9,11,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	3,10,12	2,8,9,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	3,10,12,16,17,18	2,8,9,11,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	3,10,12,14,17	2,8,9,11,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	3,10,12,14,16,18	2,8,9,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	3,10,12,14,17,18	2,8,9,11,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	3,10,12,14,16	2,8,9,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	3,10,12	2,8,9,11,13	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	3,10,12,16,17,18	2,8,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	3,10,12,18	2,8,9,11,13,15,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	3,10,12,16,17	2,8,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	3,10,12,14,17,18	2,8,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	3,10,12,14,16	2,8,9,11,13	2^{-12}
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	3,10,12,14,17	2,8,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	3,10,12,14,16,18	2,8,9,11,13,15,18	2^{-12}

Table 0.785 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	3,7,17,18	2,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	3,7,16	2	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	3,7,17	2,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	3,7,16,18	2,15,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	3,7,14	2	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	3,7,14,16,17,18	2,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	3,7,14,18	2,15,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	3,7,14,16,17	2,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	3,7,17	2,13,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	3,7,16,18	2,13,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	3,7,17,18	2,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	3,7,16	2,13,15	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,7,14,18	2,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	3,7,14,16,17	2,13,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	3,7,14	2,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	3,7,14,16,17,18	2,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	3,7,12	2	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	3,7,12,16,17,18	2,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	3,7,12,18	2,15,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	3,7,12,16,17	2,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	3,7,12,14,17,18	2,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	3,7,12,14,16	2	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	3,7,12,14,17	2,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	3,7,12,14,16,18	2,15,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	3,7,12,18	2,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	3,7,12,16,17	2,13,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	3,7,12	2,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	3,7,12,16,17,18	2,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	3,7,12,14,17	2,13,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	3,7,12,14,16,18	2,13,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	3,7,12,14,17,18	2,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	3,7,12,14,16	2,13,15	$2^{-28.5}$

Table 0.786 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	3,7,17	2,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	3,7,16,18	2,11,18	2^{-34}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	3,7,17,18	2,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	3,7,16	2,11,15	2^{-34}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	3,7,14,18	2,11,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	3,7,14,16,17	2,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	3,7,14	2,11,15	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	3,7,14,16,17,18	2,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	3,7,17,18	2,11,13,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	3,7,16	2,11,13	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	3,7,17	2,11,13,15,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	3,7,16,18	2,11,13,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	3,7,14	2,11,13	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	3,7,14,16,17,18	2,11,13,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	3,7,14,18	2,11,13,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	3,7,14,16,17	2,11,13,15,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	3,7,12,18	2,11,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	3,7,12,16,17	2,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	3,7,12	2,11,15	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	3,7,12,16,17,18	2,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	3,7,12,14,17	2,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	3,7,12,14,16,18	2,11,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	3,7,12,14,17,18	2,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	3,7,12,14,16	2,11,15	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	3,7,12	2,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	3,7,12,16,17,18	2,11,13,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	3,7,12,18	2,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	3,7,12,16,17	2,11,13,15,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	3,7,12,14,17,18	2,11,13,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	3,7,12,14,16	2,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	3,7,12,14,17	2,11,13,15,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	3,7,12,14,16,18	2,11,13,15,18	$2^{-17.5}$

Table 0.787 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	3,7,10	2	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	3,7,10,16,17,18	2,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	3,7,10,18	2,15,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	3,7,10,16,17	2,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,7,10,14,17,18	2,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	3,7,10,14,16	2	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	3,7,10,14,17	2,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	3,7,10,14,16,18	2,15,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	3,7,10,18	2,13,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	3,7,10,16,17	2,13,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	3,7,10	2,13,15	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	3,7,10,16,17,18	2,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,7,10,14,17	2,13,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	3,7,10,14,16,18	2,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	3,7,10,14,17,18	2,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	3,7,10,14,16	2,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	3,7,10,12,17,18	2,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	3,7,10,12,16	2	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,7,10,12,17	2,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	3,7,10,12,16,18	2,15,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	3,7,10,12,14	2	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	3,7,10,12,14,16,17,18	2,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	3,7,10,12,14,18	2,15,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	3,7,10,12,14,16,17	2,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	3,7,10,12,17	2,13,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	3,7,10,12,16,18	2,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	3,7,10,12,17,18	2,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	3,7,10,12,16	2,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	3,7,10,12,14,18	2,13,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	3,7,10,12,14,16,17	2,13,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	3,7,10,12,14	2,13,15	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	3,7,10,12,14,16,17,18	2,13,15,17,18	2^{-12}

Table 0.788 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	3,7,10,18	2,11,18	2^{-1}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	3,7,10,16,17	2,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,7,10	2,11,15	2^{-1}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,7,10,16,17,18	2,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	3,7,10,14,17	2,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	3,7,10,14,16,18	2,11,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	3,7,10,14,17,18	2,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	3,7,10,14,16	2,11,15	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	3,7,10	2,11,13	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	3,7,10,16,17,18	2,11,13,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	3,7,10,18	2,11,13,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	3,7,10,16,17	2,11,13,15,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	3,7,10,14,17,18	2,11,13,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	3,7,10,14,16	2,11,13	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	3,7,10,14,17	2,11,13,15,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	3,7,10,14,16,18	2,11,13,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	3,7,10,12,17	2,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	3,7,10,12,16,18	2,11,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	3,7,10,12,17,18	2,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	3,7,10,12,16	2,11,15	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	3,7,10,12,14,18	2,11,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	3,7,10,12,14,16,17	2,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	3,7,10,12,14	2,11,15	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	3,7,10,12,14,16,17,18	2,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,7,10,12,17,18	2,11,13,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	3,7,10,12,16	2,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	3,7,10,12,17	2,11,13,15,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	3,7,10,12,16,18	2,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	3,7,10,12,14	2,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	3,7,10,12,14,16,17,18	2,11,13,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	3,7,10,12,14,18	2,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	3,7,10,12,14,16,17	2,11,13,15,17	2^{-23}

Table 0.789 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	3,7,17	2,9,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	3,7,16,18	2,9,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	3,7,17,18	2,9,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	3,7,16	2,9,15	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	3,7,14,18	2,9,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	3,7,14,16,17	2,9,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	3,7,14	2,9,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	3,7,14,16,17,18	2,9,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	3,7,17,18	2,9,13,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	3,7,16	2,9,13	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	3,7,17	2,9,13,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	3,7,16,18	2,9,13,15,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	3,7,14	2,9,13	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	3,7,14,16,17,18	2,9,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	3,7,14,18	2,9,13,15,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	3,7,14,16,17	2,9,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	3,7,12,18	2,9,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	3,7,12,16,17	2,9,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	3,7,12	2,9,15	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	3,7,12,16,17,18	2,9,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	3,7,12,14,17	2,9,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	3,7,12,14,16,18	2,9,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	3,7,12,14,17,18	2,9,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	3,7,12,14,16	2,9,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	3,7,12	2,9,13	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	3,7,12,16,17,18	2,9,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	3,7,12,18	2,9,13,15,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	3,7,12,16,17	2,9,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	3,7,12,14,17,18	2,9,13,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	3,7,12,14,16	2,9,13	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	3,7,12,14,17	2,9,13,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	3,7,12,14,16,18	2,9,13,15,18	2^{-12}

Table 0.790 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	3,7,17,18	2,9,11,17,18	2^{-1}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	3,7,16	2,9,11	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	3,7,17	2,9,11,15,17	2^{-1}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	3,7,16,18	2,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	3,7,14	2,9,11	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,7,14,16,17,18	2,9,11,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	3,7,14,18	2,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	3,7,14,16,17	2,9,11,15,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	3,7,17	2,9,11,13,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	3,7,16,18	2,9,11,13,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	3,7,17,18	2,9,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,7,16	2,9,11,13,15	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	3,7,14,18	2,9,11,13,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,7,14,16,17	2,9,11,13,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	3,7,14	2,9,11,13,15	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	3,7,14,16,17,18	2,9,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	3,7,12	2,9,11	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	3,7,12,16,17,18	2,9,11,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	3,7,12,18	2,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	3,7,12,16,17	2,9,11,15,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	3,7,12,14,17,18	2,9,11,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	3,7,12,14,16	2,9,11	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,7,12,14,17	2,9,11,15,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	3,7,12,14,16,18	2,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	3,7,12,18	2,9,11,13,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	3,7,12,16,17	2,9,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	3,7,12	2,9,11,13,15	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	3,7,12,16,17,18	2,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	3,7,12,14,17	2,9,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	3,7,12,14,16,18	2,9,11,13,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	3,7,12,14,17,18	2,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	3,7,12,14,16	2,9,11,13,15	2^{-23}

Table 0.791 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	3,7,10,18	2,9,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	3,7,10,16,17	2,9,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	3,7,10	2,9,15	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	3,7,10,16,17,18	2,9,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	3,7,10,14,17	2,9,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	3,7,10,14,16,18	2,9,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	3,7,10,14,17,18	2,9,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	3,7,10,14,16	2,9,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	3,7,10	2,9,13	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	3,7,10,16,17,18	2,9,13,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	3,7,10,18	2,9,13,15,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	3,7,10,16,17	2,9,13,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	3,7,10,14,17,18	2,9,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	3,7,10,14,16	2,9,13	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	3,7,10,14,17	2,9,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	3,7,10,14,16,18	2,9,13,15,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	3,7,10,12,17	2,9,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	3,7,10,12,16,18	2,9,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	3,7,10,12,17,18	2,9,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	3,7,10,12,16	2,9,15	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	3,7,10,12,14,18	2,9,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	3,7,10,12,14,16,17	2,9,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	3,7,10,12,14	2,9,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	3,7,10,12,14,16,17,18	2,9,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	3,7,10,12,17,18	2,9,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	3,7,10,12,16	2,9,13	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	3,7,10,12,17	2,9,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	3,7,10,12,16,18	2,9,13,15,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	3,7,10,12,14	2,9,13	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	3,7,10,12,14,16,17,18	2,9,13,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	3,7,10,12,14,18	2,9,13,15,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	3,7,10,12,14,16,17	2,9,13,15,17	$2^{-28.5}$

Table 0.792 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	3,7,10	2,9,11	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	3,7,10,16,17,18	2,9,11,17,18	2^{-34}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	3,7,10,18	2,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	3,7,10,16,17	2,9,11,15,17	2^{-34}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	3,7,10,14,17,18	2,9,11,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	3,7,10,14,16	2,9,11	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,7,10,14,17	2,9,11,15,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	3,7,10,14,16,18	2,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	3,7,10,18	2,9,11,13,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	3,7,10,16,17	2,9,11,13,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	3,7,10	2,9,11,13,15	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	3,7,10,16,17,18	2,9,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	3,7,10,14,17	2,9,11,13,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	3,7,10,14,16,18	2,9,11,13,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	3,7,10,14,17,18	2,9,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	3,7,10,14,16	2,9,11,13,15	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	3,7,10,12,17,18	2,9,11,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	3,7,10,12,16	2,9,11	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	3,7,10,12,17	2,9,11,15,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	3,7,10,12,16,18	2,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	3,7,10,12,14	2,9,11	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	3,7,10,12,14,16,17,18	2,9,11,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	3,7,10,12,14,18	2,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	3,7,10,12,14,16,17	2,9,11,15,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	3,7,10,12,17	2,9,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	3,7,10,12,16,18	2,9,11,13,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	3,7,10,12,17,18	2,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	3,7,10,12,16	2,9,11,13,15	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	3,7,10,12,14,18	2,9,11,13,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,7,10,12,14,16,17	2,9,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	3,7,10,12,14	2,9,11,13,15	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	3,7,10,12,14,16,17,18	2,9,11,13,15,17,18	$2^{-17.5}$

Table 0.793 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	3,7	2,8	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	3,7,16,17,18	2,8,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	3,7,18	2,8,15,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	3,7,16,17	2,8,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	3,7,14,17,18	2,8,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	3,7,14,16	2,8	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	3,7,14,17	2,8,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	3,7,14,16,18	2,8,15,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	3,7,18	2,8,13,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	3,7,16,17	2,8,13,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	3,7	2,8,13,15	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	3,7,16,17,18	2,8,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	3,7,14,17	2,8,13,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	3,7,14,16,18	2,8,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	3,7,14,17,18	2,8,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	3,7,14,16	2,8,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,7,12,17,18	2,8,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	3,7,12,16	2,8	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	3,7,12,17	2,8,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	3,7,12,16,18	2,8,15,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	3,7,12,14	2,8	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,7,12,14,16,17,18	2,8,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	3,7,12,14,18	2,8,15,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	3,7,12,14,16,17	2,8,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	3,7,12,17	2,8,13,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	3,7,12,16,18	2,8,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	3,7,12,17,18	2,8,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,7,12,16	2,8,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	3,7,12,14,18	2,8,13,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	3,7,12,14,16,17	2,8,13,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	3,7,12,14	2,8,13,15	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	3,7,12,14,16,17,18	2,8,13,15,17,18	2^{-23}

Table 0.794 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	3,7,18	2,8,11,18	2^{-34}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	3,7,16,17	2,8,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	3,7	2,8,11,15	2^{-34}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	3,7,16,17,18	2,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	3,7,14,17	2,8,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	3,7,14,16,18	2,8,11,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	3,7,14,17,18	2,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,7,14,16	2,8,11,15	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	3,7	2,8,11,13	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	3,7,16,17,18	2,8,11,13,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	3,7,18	2,8,11,13,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	3,7,16,17	2,8,11,13,15,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	3,7,14,17,18	2,8,11,13,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	3,7,14,16	2,8,11,13	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	3,7,14,17	2,8,11,13,15,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	3,7,14,16,18	2,8,11,13,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	3,7,12,17	2,8,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	3,7,12,16,18	2,8,11,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	3,7,12,17,18	2,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	3,7,12,16	2,8,11,15	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	3,7,12,14,18	2,8,11,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	3,7,12,14,16,17	2,8,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	3,7,12,14	2,8,11,15	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	3,7,12,14,16,17,18	2,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	3,7,12,17,18	2,8,11,13,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	3,7,12,16	2,8,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	3,7,12,17	2,8,11,13,15,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	3,7,12,16,18	2,8,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,7,12,14	2,8,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	3,7,12,14,16,17,18	2,8,11,13,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	3,7,12,14,18	2,8,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	3,7,12,14,16,17	2,8,11,13,15,17	2^{-12}

Table 0.795 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	3,7,10,17,18	2,8,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	3,7,10,16	2,8	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	3,7,10,17	2,8,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	3,7,10,16,18	2,8,15,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	3,7,10,14	2,8	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	3,7,10,14,16,17,18	2,8,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	3,7,10,14,18	2,8,15,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	3,7,10,14,16,17	2,8,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	3,7,10,17	2,8,13,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	3,7,10,16,18	2,8,13,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	3,7,10,17,18	2,8,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	3,7,10,16	2,8,13,15	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	3,7,10,14,18	2,8,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	3,7,10,14,16,17	2,8,13,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	3,7,10,14	2,8,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	3,7,10,14,16,17,18	2,8,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	3,7,10,12	2,8	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	3,7,10,12,16,17,18	2,8,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	3,7,10,12,18	2,8,15,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	3,7,10,12,16,17	2,8,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	3,7,10,12,14,17,18	2,8,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	3,7,10,12,14,16	2,8	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	3,7,10,12,14,17	2,8,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	3,7,10,12,14,16,18	2,8,15,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	3,7,10,12,18	2,8,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	3,7,10,12,16,17	2,8,13,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	3,7,10,12	2,8,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	3,7,10,12,16,17,18	2,8,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	3,7,10,12,14,17	2,8,13,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	3,7,10,12,14,16,18	2,8,13,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	3,7,10,12,14,17,18	2,8,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	3,7,10,12,14,16	2,8,13,15	$2^{-6.5}$

Table 0.796 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	3,7,10,17	2,8,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	3,7,10,16,18	2,8,11,18	2^{-1}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	3,7,10,17,18	2,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	3,7,10,16	2,8,11,15	2^{-1}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,7,10,14,18	2,8,11,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	3,7,10,14,16,17	2,8,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	3,7,10,14	2,8,11,15	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	3,7,10,14,16,17,18	2,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	3,7,10,17,18	2,8,11,13,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	3,7,10,16	2,8,11,13	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	3,7,10,17	2,8,11,13,15,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	3,7,10,16,18	2,8,11,13,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,7,10,14	2,8,11,13	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	3,7,10,14,16,17,18	2,8,11,13,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	3,7,10,14,18	2,8,11,13,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	3,7,10,14,16,17	2,8,11,13,15,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	3,7,10,12,18	2,8,11,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	3,7,10,12,16,17	2,8,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	3,7,10,12	2,8,11,15	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	3,7,10,12,16,17,18	2,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	3,7,10,12,14,17	2,8,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	3,7,10,12,14,16,18	2,8,11,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	3,7,10,12,14,17,18	2,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,7,10,12,14,16	2,8,11,15	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	3,7,10,12	2,8,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	3,7,10,12,16,17,18	2,8,11,13,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	3,7,10,12,18	2,8,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	3,7,10,12,16,17	2,8,11,13,15,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	3,7,10,12,14,17,18	2,8,11,13,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	3,7,10,12,14,16	2,8,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	3,7,10,12,14,17	2,8,11,13,15,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	3,7,10,12,14,16,18	2,8,11,13,15,18	$2^{-17.5}$

Table 0.797 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	3,7,18	2,8,9,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	3,7,16,17	2,8,9,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	3,7	2,8,9,15	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	3,7,16,17,18	2,8,9,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	3,7,14,17	2,8,9,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,7,14,16,18	2,8,9,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	3,7,14,17,18	2,8,9,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	3,7,14,16	2,8,9,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	3,7	2,8,9,13	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	3,7,16,17,18	2,8,9,13,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	3,7,18	2,8,9,13,15,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	3,7,16,17	2,8,9,13,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	3,7,14,17,18	2,8,9,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,7,14,16	2,8,9,13	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	3,7,14,17	2,8,9,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	3,7,14,16,18	2,8,9,13,15,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	3,7,12,17	2,8,9,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	3,7,12,16,18	2,8,9,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	3,7,12,17,18	2,8,9,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,7,12,16	2,8,9,15	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	3,7,12,14,18	2,8,9,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	3,7,12,14,16,17	2,8,9,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	3,7,12,14	2,8,9,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	3,7,12,14,16,17,18	2,8,9,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	3,7,12,17,18	2,8,9,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	3,7,12,16	2,8,9,13	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	3,7,12,17	2,8,9,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	3,7,12,16,18	2,8,9,13,15,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	3,7,12,14	2,8,9,13	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	3,7,12,14,16,17,18	2,8,9,13,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	3,7,12,14,18	2,8,9,13,15,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	3,7,12,14,16,17	2,8,9,13,15,17	$2^{-6.5}$

Table 0.798 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	3,7	2,8,9,11	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	3,7,16,17,18	2,8,9,11,17,18	2^{-1}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,7,18	2,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,7,16,17	2,8,9,11,15,17	2^{-1}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	3,7,14,17,18	2,8,9,11,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	3,7,14,16	2,8,9,11	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	3,7,14,17	2,8,9,11,15,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	3,7,14,16,18	2,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	3,7,18	2,8,9,11,13,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	3,7,16,17	2,8,9,11,13,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	3,7	2,8,9,11,13,15	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	3,7,16,17,18	2,8,9,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	3,7,14,17	2,8,9,11,13,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	3,7,14,16,18	2,8,9,11,13,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	3,7,14,17,18	2,8,9,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	3,7,14,16	2,8,9,11,13,15	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	3,7,12,17,18	2,8,9,11,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	3,7,12,16	2,8,9,11	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	3,7,12,17	2,8,9,11,15,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	3,7,12,16,18	2,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	3,7,12,14	2,8,9,11	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	3,7,12,14,16,17,18	2,8,9,11,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	3,7,12,14,18	2,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	3,7,12,14,16,17	2,8,9,11,15,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	3,7,12,17	2,8,9,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,7,12,16,18	2,8,9,11,13,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	3,7,12,17,18	2,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	3,7,12,16	2,8,9,11,13,15	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	3,7,12,14,18	2,8,9,11,13,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	3,7,12,14,16,17	2,8,9,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	3,7,12,14	2,8,9,11,13,15	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	3,7,12,14,16,17,18	2,8,9,11,13,15,17,18	$2^{-17.5}$

Table 0.799 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	3,7,10,17	2,8,9,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	3,7,10,16,18	2,8,9,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	3,7,10,17,18	2,8,9,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	3,7,10,16	2,8,9,15	$2^{-6.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	3,7,10,14,18	2,8,9,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	3,7,10,14,16,17	2,8,9,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	3,7,10,14	2,8,9,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	3,7,10,14,16,17,18	2,8,9,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	3,7,10,17,18	2,8,9,13,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	3,7,10,16	2,8,9,13	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	3,7,10,17	2,8,9,13,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	3,7,10,16,18	2,8,9,13,15,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	3,7,10,14	2,8,9,13	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	3,7,10,14,16,17,18	2,8,9,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	3,7,10,14,18	2,8,9,13,15,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,7,10,14,16,17	2,8,9,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	3,7,10,12,18	2,8,9,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	3,7,10,12,16,17	2,8,9,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	3,7,10,12	2,8,9,15	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	3,7,10,12,16,17,18	2,8,9,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	3,7,10,12,14,17	2,8,9,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	3,7,10,12,14,16,18	2,8,9,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	3,7,10,12,14,17,18	2,8,9,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	3,7,10,12,14,16	2,8,9,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	3,7,10,12	2,8,9,13	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	3,7,10,12,16,17,18	2,8,9,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	3,7,10,12,18	2,8,9,13,15,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	3,7,10,12,16,17	2,8,9,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	3,7,10,12,14,17,18	2,8,9,13,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	3,7,10,12,14,16	2,8,9,13	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	3,7,10,12,14,17	2,8,9,13,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	3,7,10,12,14,16,18	2,8,9,13,15,18	2^{-23}

Table 0.800 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	3,7,10,17,18	2,8,9,11,17,18	2^{-34}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	3,7,10,16	2,8,9,11	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	3,7,10,17	2,8,9,11,15,17	2^{-34}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	3,7,10,16,18	2,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	3,7,10,14	2,8,9,11	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	3,7,10,14,16,17,18	2,8,9,11,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	3,7,10,14,18	2,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	3,7,10,14,16,17	2,8,9,11,15,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	3,7,10,17	2,8,9,11,13,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	3,7,10,16,18	2,8,9,11,13,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	3,7,10,17,18	2,8,9,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	3,7,10,16	2,8,9,11,13,15	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	3,7,10,14,18	2,8,9,11,13,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	3,7,10,14,16,17	2,8,9,11,13,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	3,7,10,14	2,8,9,11,13,15	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	3,7,10,14,16,17,18	2,8,9,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	3,7,10,12	2,8,9,11	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	3,7,10,12,16,17,18	2,8,9,11,17,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	3,7,10,12,18	2,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	3,7,10,12,16,17	2,8,9,11,15,17	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	3,7,10,12,14,17,18	2,8,9,11,17,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	3,7,10,12,14,16	2,8,9,11	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	3,7,10,12,14,17	2,8,9,11,15,17	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	3,7,10,12,14,16,18	2,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	3,7,10,12,18	2,8,9,11,13,18	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	3,7,10,12,16,17	2,8,9,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	3,7,10,12	2,8,9,11,13,15	2^{-23}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	3,7,10,12,16,17,18	2,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	3,7,10,12,14,17	2,8,9,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	3,7,10,12,14,16,18	2,8,9,11,13,18	2^{-12}
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	3,7,10,12,14,17,18	2,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	3,7,10,12,14,16	2,8,9,11,13,15	2^{-12}

Table 0.801 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	3,18	2,6,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	3,16,17	2,6,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	3	2,6,15	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	3,16,17,18	2,6,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	3,14,17	2,6,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	3,14,16,18	2,6,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	3,14,17,18	2,6,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	3,14,16	2,6,15	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	3	2,6,13	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	3,16,17,18	2,6,13,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	3,18	2,6,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,16,17	2,6,13,15,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	3,14,17,18	2,6,13,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	3,14,16	2,6,13	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	3,14,17	2,6,13,15,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	3,14,16,18	2,6,13,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,12,17	2,6,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	3,12,16,18	2,6,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	3,12,17,18	2,6,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	3,12,16	2,6,15	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	3,12,14,18	2,6,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	3,12,14,16,17	2,6,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	3,12,14	2,6,15	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	3,12,14,16,17,18	2,6,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	3,12,17,18	2,6,13,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	3,12,16	2,6,13	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	3,12,17	2,6,13,15,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	3,12,16,18	2,6,13,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	3,12,14	2,6,13	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	3,12,14,16,17,18	2,6,13,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	3,12,14,18	2,6,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	3,12,14,16,17	2,6,13,15,17	2^{-23}

Table 0.802 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	3	2,6,11	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	3,16,17,18	2,6,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,18	2,6,11,15,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	3,16,17	2,6,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	3,14,17,18	2,6,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	3,14,16	2,6,11	2^{-34}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	3,14,17	2,6,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	3,14,16,18	2,6,11,15,18	2^{-34}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	3,18	2,6,11,13,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	3,16,17	2,6,11,13,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	3	2,6,11,13,15	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	3,16,17,18	2,6,11,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	3,14,17	2,6,11,13,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	3,14,16,18	2,6,11,13,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	3,14,17,18	2,6,11,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	3,14,16	2,6,11,13,15	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	3,12,17,18	2,6,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	3,12,16	2,6,11	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	3,12,17	2,6,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	3,12,16,18	2,6,11,15,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	3,12,14	2,6,11	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	3,12,14,16,17,18	2,6,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	3,12,14,18	2,6,11,15,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	3,12,14,16,17	2,6,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	3,12,17	2,6,11,13,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	3,12,16,18	2,6,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	3,12,17,18	2,6,11,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	3,12,16	2,6,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	3,12,14,18	2,6,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	3,12,14,16,17	2,6,11,13,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	3,12,14	2,6,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	3,12,14,16,17,18	2,6,11,13,15,17,18	2^{-23}

Table 0.803 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(2)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,10,17	2,6,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	3,10,16,18	2,6,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	3,10,17,18	2,6,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	3,10,16	2,6,15	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	3,10,14,18	2,6,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	3,10,14,16,17	2,6,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	3,10,14	2,6,15	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	3,10,14,16,17,18	2,6,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	3,10,17,18	2,6,13,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	3,10,16	2,6,13	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	3,10,17	2,6,13,15,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	3,10,16,18	2,6,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	3,10,14	2,6,13	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	3,10,14,16,17,18	2,6,13,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	3,10,14,18	2,6,13,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	3,10,14,16,17	2,6,13,15,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	3,10,12,18	2,6,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	3,10,12,16,17	2,6,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	3,10,12	2,6,15	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,10,12,16,17,18	2,6,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	3,10,12,14,17	2,6,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	3,10,12,14,16,18	2,6,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	3,10,12,14,17,18	2,6,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	3,10,12,14,16	2,6,15	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	3,10,12	2,6,13	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	3,10,12,16,17,18	2,6,13,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	3,10,12,18	2,6,13,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,10,12,16,17	2,6,13,15,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	3,10,12,14,17,18	2,6,13,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	3,10,12,14,16	2,6,13	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	3,10,12,14,17	2,6,13,15,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	3,10,12,14,16,18	2,6,13,15,18	$2^{-17.5}$

Table 0.804 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	3,10,17,18	2,6,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	3,10,16	2,6,11	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	3,10,17	2,6,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	3,10,16,18	2,6,11,15,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	3,10,14	2,6,11	2^{-1}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	3,10,14,16,17,18	2,6,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	3,10,14,18	2,6,11,15,18	2^{-1}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	3,10,14,16,17	2,6,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,10,17	2,6,11,13,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	3,10,16,18	2,6,11,13,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	3,10,17,18	2,6,11,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	3,10,16	2,6,11,13,15	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	3,10,14,18	2,6,11,13,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	3,10,14,16,17	2,6,11,13,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	3,10,14	2,6,11,13,15	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	3,10,14,16,17,18	2,6,11,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	3,10,12	2,6,11	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	3,10,12,16,17,18	2,6,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	3,10,12,18	2,6,11,15,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	3,10,12,16,17	2,6,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	3,10,12,14,17,18	2,6,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	3,10,12,14,16	2,6,11	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	3,10,12,14,17	2,6,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	3,10,12,14,16,18	2,6,11,15,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	3,10,12,18	2,6,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	3,10,12,16,17	2,6,11,13,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	3,10,12	2,6,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	3,10,12,16,17,18	2,6,11,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	3,10,12,14,17	2,6,11,13,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	3,10,12,14,16,18	2,6,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	3,10,12,14,17,18	2,6,11,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	3,10,12,14,16	2,6,11,13,15	$2^{-17.5}$

Table 0.805 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	3	2,6,9	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	3,16,17,18	2,6,9,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	3,18	2,6,9,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	3,16,17	2,6,9,15,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	3,14,17,18	2,6,9,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	3,14,16	2,6,9	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	3,14,17	2,6,9,15,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	3,14,16,18	2,6,9,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	3,18	2,6,9,13,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	3,16,17	2,6,9,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	3	2,6,9,13,15	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	3,16,17,18	2,6,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	3,14,17	2,6,9,13,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	3,14,16,18	2,6,9,13,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,14,17,18	2,6,9,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	3,14,16	2,6,9,13,15	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	3,12,17,18	2,6,9,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	3,12,16	2,6,9	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	3,12,17	2,6,9,15,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	3,12,16,18	2,6,9,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,12,14	2,6,9	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,12,14,16,17,18	2,6,9,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	3,12,14,18	2,6,9,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	3,12,14,16,17	2,6,9,15,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	3,12,17	2,6,9,13,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	3,12,16,18	2,6,9,13,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	3,12,17,18	2,6,9,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	3,12,16	2,6,9,13,15	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	3,12,14,18	2,6,9,13,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	3,12,14,16,17	2,6,9,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	3,12,14	2,6,9,13,15	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	3,12,14,16,17,18	2,6,9,13,15,17,18	$2^{-17.5}$

Table 0.806 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	3,18	2,6,9,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	3,16,17	2,6,9,11,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	3	2,6,9,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	3,16,17,18	2,6,9,11,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,14,17	2,6,9,11,17	2^{-1}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	3,14,16,18	2,6,9,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	3,14,17,18	2,6,9,11,15,17,18	2^{-1}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	3,14,16	2,6,9,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	3	2,6,9,11,13	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	3,16,17,18	2,6,9,11,13,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	3,18	2,6,9,11,13,15,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	3,16,17	2,6,9,11,13,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	3,14,17,18	2,6,9,11,13,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	3,14,16	2,6,9,11,13	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	3,14,17	2,6,9,11,13,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	3,14,16,18	2,6,9,11,13,15,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	3,12,17	2,6,9,11,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	3,12,16,18	2,6,9,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,12,17,18	2,6,9,11,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	3,12,16	2,6,9,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	3,12,14,18	2,6,9,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	3,12,14,16,17	2,6,9,11,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	3,12,14	2,6,9,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	3,12,14,16,17,18	2,6,9,11,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	3,12,17,18	2,6,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	3,12,16	2,6,9,11,13	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,12,17	2,6,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	3,12,16,18	2,6,9,11,13,15,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	3,12,14	2,6,9,11,13	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	3,12,14,16,17,18	2,6,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	3,12,14,18	2,6,9,11,13,15,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	3,12,14,16,17	2,6,9,11,13,15,17	$2^{-17.5}$

Table 0.807 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	3,10,17,18	2,6,9,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	3,10,16	2,6,9	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	3,10,17	2,6,9,15,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	3,10,16,18	2,6,9,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	3,10,14	2,6,9	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	3,10,14,16,17,18	2,6,9,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	3,10,14,18	2,6,9,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	3,10,14,16,17	2,6,9,15,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	3,10,17	2,6,9,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	3,10,16,18	2,6,9,13,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	3,10,17,18	2,6,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	3,10,16	2,6,9,13,15	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	3,10,14,18	2,6,9,13,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	3,10,14,16,17	2,6,9,13,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	3,10,14	2,6,9,13,15	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	3,10,14,16,17,18	2,6,9,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	3,10,12	2,6,9	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	3,10,12,16,17,18	2,6,9,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	3,10,12,18	2,6,9,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	3,10,12,16,17	2,6,9,15,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	3,10,12,14,17,18	2,6,9,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	3,10,12,14,16	2,6,9	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	3,10,12,14,17	2,6,9,15,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	3,10,12,14,16,18	2,6,9,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	3,10,12,18	2,6,9,13,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	3,10,12,16,17	2,6,9,13,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	3,10,12	2,6,9,13,15	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	3,10,12,16,17,18	2,6,9,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	3,10,12,14,17	2,6,9,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	3,10,12,14,16,18	2,6,9,13,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	3,10,12,14,17,18	2,6,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	3,10,12,14,16	2,6,9,13,15	2^{-23}

Table 0.808 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	3,10,17	2,6,9,11,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	3,10,16,18	2,6,9,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	3,10,17,18	2,6,9,11,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	3,10,16	2,6,9,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	3,10,14,18	2,6,9,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	3,10,14,16,17	2,6,9,11,17	2^{-34}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	3,10,14	2,6,9,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	3,10,14,16,17,18	2,6,9,11,15,17,18	2^{-34}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	3,10,17,18	2,6,9,11,13,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	3,10,16	2,6,9,11,13	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	3,10,17	2,6,9,11,13,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	3,10,16,18	2,6,9,11,13,15,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	3,10,14	2,6,9,11,13	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	3,10,14,16,17,18	2,6,9,11,13,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	3,10,14,18	2,6,9,11,13,15,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	3,10,14,16,17	2,6,9,11,13,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	3,10,12,18	2,6,9,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	3,10,12,16,17	2,6,9,11,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	3,10,12	2,6,9,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	3,10,12,16,17,18	2,6,9,11,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	3,10,12,14,17	2,6,9,11,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	3,10,12,14,16,18	2,6,9,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	3,10,12,14,17,18	2,6,9,11,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	3,10,12,14,16	2,6,9,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	3,10,12	2,6,9,11,13	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	3,10,12,16,17,18	2,6,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,10,12,18	2,6,9,11,13,15,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	3,10,12,16,17	2,6,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	3,10,12,14,17,18	2,6,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	3,10,12,14,16	2,6,9,11,13	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	3,10,12,14,17	2,6,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	3,10,12,14,16,18	2,6,9,11,13,15,18	2^{-23}

Table 0.809 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	3,17	2,6,8,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	3,16,18	2,6,8,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	3,17,18	2,6,8,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	3,16	2,6,8,15	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	3,14,18	2,6,8,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	3,14,16,17	2,6,8,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	3,14	2,6,8,15	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	3,14,16,17,18	2,6,8,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	3,17,18	2,6,8,13,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	3,16	2,6,8,13	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	3,17	2,6,8,13,15,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	3,16,18	2,6,8,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	3,14	2,6,8,13	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	3,14,16,17,18	2,6,8,13,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	3,14,18	2,6,8,13,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	3,14,16,17	2,6,8,13,15,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	3,12,18	2,6,8,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	3,12,16,17	2,6,8,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	3,12	2,6,8,15	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	3,12,16,17,18	2,6,8,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	3,12,14,17	2,6,8,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	3,12,14,16,18	2,6,8,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	3,12,14,17,18	2,6,8,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	3,12,14,16	2,6,8,15	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	3,12	2,6,8,13	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	3,12,16,17,18	2,6,8,13,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	3,12,18	2,6,8,13,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	3,12,16,17	2,6,8,13,15,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	3,12,14,17,18	2,6,8,13,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	3,12,14,16	2,6,8,13	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	3,12,14,17	2,6,8,13,15,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	3,12,14,16,18	2,6,8,13,15,18	$2^{-17.5}$

Table 0.810 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	3,17,18	2,6,8,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	3,16	2,6,8,11	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	3,17	2,6,8,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	3,16,18	2,6,8,11,15,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	3,14	2,6,8,11	2^{-34}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	3,14,16,17,18	2,6,8,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	3,14,18	2,6,8,11,15,18	2^{-34}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	3,14,16,17	2,6,8,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	3,17	2,6,8,11,13,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	3,16,18	2,6,8,11,13,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	3,17,18	2,6,8,11,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	3,16	2,6,8,11,13,15	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	3,14,18	2,6,8,11,13,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	3,14,16,17	2,6,8,11,13,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	3,14	2,6,8,11,13,15	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	3,14,16,17,18	2,6,8,11,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	3,12	2,6,8,11	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	3,12,16,17,18	2,6,8,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	3,12,18	2,6,8,11,15,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	3,12,16,17	2,6,8,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	3,12,14,17,18	2,6,8,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	3,12,14,16	2,6,8,11	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	3,12,14,17	2,6,8,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	3,12,14,16,18	2,6,8,11,15,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	3,12,18	2,6,8,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	3,12,16,17	2,6,8,11,13,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	3,12	2,6,8,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,12,16,17,18	2,6,8,11,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	3,12,14,17	2,6,8,11,13,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	3,12,14,16,18	2,6,8,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	3,12,14,17,18	2,6,8,11,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	3,12,14,16	2,6,8,11,13,15	$2^{-17.5}$

Table 0.811 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	3,10,18	2,6,8,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	3,10,16,17	2,6,8,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	3,10	2,6,8,15	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	3,10,16,17,18	2,6,8,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	3,10,14,17	2,6,8,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	3,10,14,16,18	2,6,8,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	3,10,14,17,18	2,6,8,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	3,10,14,16	2,6,8,15	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	3,10	2,6,8,13	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	3,10,16,17,18	2,6,8,13,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	3,10,18	2,6,8,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	3,10,16,17	2,6,8,13,15,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	3,10,14,17,18	2,6,8,13,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	3,10,14,16	2,6,8,13	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	3,10,14,17	2,6,8,13,15,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,10,14,16,18	2,6,8,13,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	3,10,12,17	2,6,8,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	3,10,12,16,18	2,6,8,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	3,10,12,17,18	2,6,8,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	3,10,12,16	2,6,8,15	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,10,12,14,18	2,6,8,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,10,12,14,16,17	2,6,8,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	3,10,12,14	2,6,8,15	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	3,10,12,14,16,17,18	2,6,8,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	3,10,12,17,18	2,6,8,13,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	3,10,12,16	2,6,8,13	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	3,10,12,17	2,6,8,13,15,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	3,10,12,16,18	2,6,8,13,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	3,10,12,14	2,6,8,13	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	3,10,12,14,16,17,18	2,6,8,13,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	3,10,12,14,18	2,6,8,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	3,10,12,14,16,17	2,6,8,13,15,17	2^{-12}

Table 0.812 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	3,10	2,6,8,11	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	3,10,16,17,18	2,6,8,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	3,10,18	2,6,8,11,15,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	3,10,16,17	2,6,8,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	3,10,14,17,18	2,6,8,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,10,14,16	2,6,8,11	2^{-1}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	3,10,14,17	2,6,8,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	3,10,14,16,18	2,6,8,11,15,18	2^{-1}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	3,10,18	2,6,8,11,13,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	3,10,16,17	2,6,8,11,13,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	3,10	2,6,8,11,13,15	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	3,10,16,17,18	2,6,8,11,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	3,10,14,17	2,6,8,11,13,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	3,10,14,16,18	2,6,8,11,13,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	3,10,14,17,18	2,6,8,11,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	3,10,14,16	2,6,8,11,13,15	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	3,10,12,17,18	2,6,8,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	3,10,12,16	2,6,8,11	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	3,10,12,17	2,6,8,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,10,12,16,18	2,6,8,11,15,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	3,10,12,14	2,6,8,11	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	3,10,12,14,16,17,18	2,6,8,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	3,10,12,14,18	2,6,8,11,15,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	3,10,12,14,16,17	2,6,8,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	3,10,12,17	2,6,8,11,13,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	3,10,12,16,18	2,6,8,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	3,10,12,17,18	2,6,8,11,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,10,12,16	2,6,8,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	3,10,12,14,18	2,6,8,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	3,10,12,14,16,17	2,6,8,11,13,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	3,10,12,14	2,6,8,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	3,10,12,14,16,17,18	2,6,8,11,13,15,17,18	2^{-12}

Table 0.813 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	3,17,18	2,6,8,9,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,16	2,6,8,9	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	3,17	2,6,8,9,15,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	3,16,18	2,6,8,9,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	3,14	2,6,8,9	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	3,14,16,17,18	2,6,8,9,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	3,14,18	2,6,8,9,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	3,14,16,17	2,6,8,9,15,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	3,17	2,6,8,9,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	3,16,18	2,6,8,9,13,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	3,17,18	2,6,8,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	3,16	2,6,8,9,13,15	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	3,14,18	2,6,8,9,13,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	3,14,16,17	2,6,8,9,13,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	3,14	2,6,8,9,13,15	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	3,14,16,17,18	2,6,8,9,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	3,12	2,6,8,9	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	3,12,16,17,18	2,6,8,9,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,12,18	2,6,8,9,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	3,12,16,17	2,6,8,9,15,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	3,12,14,17,18	2,6,8,9,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	3,12,14,16	2,6,8,9	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	3,12,14,17	2,6,8,9,15,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	3,12,14,16,18	2,6,8,9,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	3,12,18	2,6,8,9,13,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	3,12,16,17	2,6,8,9,13,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,12	2,6,8,9,13,15	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	3,12,16,17,18	2,6,8,9,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	3,12,14,17	2,6,8,9,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	3,12,14,16,18	2,6,8,9,13,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	3,12,14,17,18	2,6,8,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,12,14,16	2,6,8,9,13,15	2^{-12}

Table 0.814 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	3,17	2,6,8,9,11,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	3,16,18	2,6,8,9,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	3,17,18	2,6,8,9,11,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	3,16	2,6,8,9,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	3,14,18	2,6,8,9,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	3,14,16,17	2,6,8,9,11,17	2^{-1}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	3,14	2,6,8,9,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	3,14,16,17,18	2,6,8,9,11,15,17,18	2^{-1}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	3,17,18	2,6,8,9,11,13,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,16	2,6,8,9,11,13	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	3,17	2,6,8,9,11,13,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	3,16,18	2,6,8,9,11,13,15,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	3,14	2,6,8,9,11,13	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	3,14,16,17,18	2,6,8,9,11,13,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	3,14,18	2,6,8,9,11,13,15,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	3,14,16,17	2,6,8,9,11,13,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	3,12,18	2,6,8,9,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	3,12,16,17	2,6,8,9,11,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	3,12	2,6,8,9,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	3,12,16,17,18	2,6,8,9,11,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	3,12,14,17	2,6,8,9,11,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	3,12,14,16,18	2,6,8,9,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	3,12,14,17,18	2,6,8,9,11,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	3,12,14,16	2,6,8,9,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	3,12	2,6,8,9,11,13	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	3,12,16,17,18	2,6,8,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	3,12,18	2,6,8,9,11,13,15,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	3,12,16,17	2,6,8,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	3,12,14,17,18	2,6,8,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	3,12,14,16	2,6,8,9,11,13	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	3,12,14,17	2,6,8,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	3,12,14,16,18	2,6,8,9,11,13,15,18	2^{-12}

Table 0.815 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	3,10	2,6,8,9	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	3,10,16,17,18	2,6,8,9,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	3,10,18	2,6,8,9,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	3,10,16,17	2,6,8,9,15,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	3,10,14,17,18	2,6,8,9,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	3,10,14,16	2,6,8,9	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	3,10,14,17	2,6,8,9,15,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	3,10,14,16,18	2,6,8,9,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	3,10,18	2,6,8,9,13,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	3,10,16,17	2,6,8,9,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,10	2,6,8,9,13,15	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	3,10,16,17,18	2,6,8,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	3,10,14,17	2,6,8,9,13,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	3,10,14,16,18	2,6,8,9,13,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	3,10,14,17,18	2,6,8,9,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	3,10,14,16	2,6,8,9,13,15	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	3,10,12,17,18	2,6,8,9,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,10,12,16	2,6,8,9	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	3,10,12,17	2,6,8,9,15,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	3,10,12,16,18	2,6,8,9,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	3,10,12,14	2,6,8,9	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	3,10,12,14,16,17,18	2,6,8,9,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	3,10,12,14,18	2,6,8,9,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	3,10,12,14,16,17	2,6,8,9,15,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	3,10,12,17	2,6,8,9,13,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	3,10,12,16,18	2,6,8,9,13,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	3,10,12,17,18	2,6,8,9,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	3,10,12,16	2,6,8,9,13,15	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	3,10,12,14,18	2,6,8,9,13,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	3,10,12,14,16,17	2,6,8,9,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	3,10,12,14	2,6,8,9,13,15	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	3,10,12,14,16,17,18	2,6,8,9,13,15,17,18	$2^{-17.5}$

Table 0.816 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	3,10,18	2,6,8,9,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	3,10,16,17	2,6,8,9,11,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	3,10	2,6,8,9,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,10,16,17,18	2,6,8,9,11,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	3,10,14,17	2,6,8,9,11,17	2^{-34}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	3,10,14,16,18	2,6,8,9,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	3,10,14,17,18	2,6,8,9,11,15,17,18	2^{-34}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	3,10,14,16	2,6,8,9,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	3,10	2,6,8,9,11,13	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	3,10,16,17,18	2,6,8,9,11,13,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	3,10,18	2,6,8,9,11,13,15,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	3,10,16,17	2,6,8,9,11,13,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	3,10,14,17,18	2,6,8,9,11,13,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	3,10,14,16	2,6,8,9,11,13	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	3,10,14,17	2,6,8,9,11,13,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	3,10,14,16,18	2,6,8,9,11,13,15,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	3,10,12,17	2,6,8,9,11,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	3,10,12,16,18	2,6,8,9,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	3,10,12,17,18	2,6,8,9,11,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	3,10,12,16	2,6,8,9,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	3,10,12,14,18	2,6,8,9,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	3,10,12,14,16,17	2,6,8,9,11,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	3,10,12,14	2,6,8,9,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	3,10,12,14,16,17,18	2,6,8,9,11,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	3,10,12,17,18	2,6,8,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	3,10,12,16	2,6,8,9,11,13	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	3,10,12,17	2,6,8,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	3,10,12,16,18	2,6,8,9,11,13,15,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	3,10,12,14	2,6,8,9,11,13	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	3,10,12,14,16,17,18	2,6,8,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	3,10,12,14,18	2,6,8,9,11,13,15,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	3,10,12,14,16,17	2,6,8,9,11,13,15,17	$2^{-17.5}$

Table 0.817 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	3,7	2,6	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	3,7,16,17,18	2,6,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	3,7,18	2,6,15,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	3,7,16,17	2,6,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	3,7,14,17,18	2,6,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	3,7,14,16	2,6	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,7,14,17	2,6,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	3,7,14,16,18	2,6,15,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	3,7,18	2,6,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	3,7,16,17	2,6,13,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	3,7	2,6,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	3,7,16,17,18	2,6,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	3,7,14,17	2,6,13,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	3,7,14,16,18	2,6,13,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	3,7,14,17,18	2,6,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	3,7,14,16	2,6,13,15	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,7,12,17,18	2,6,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	3,7,12,16	2,6	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	3,7,12,17	2,6,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	3,7,12,16,18	2,6,15,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	3,7,12,14	2,6	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	3,7,12,14,16,17,18	2,6,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	3,7,12,14,18	2,6,15,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	3,7,12,14,16,17	2,6,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,7,12,17	2,6,13,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	3,7,12,16,18	2,6,13,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	3,7,12,17,18	2,6,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	3,7,12,16	2,6,13,15	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	3,7,12,14,18	2,6,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	3,7,12,14,16,17	2,6,13,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	3,7,12,14	2,6,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	3,7,12,14,16,17,18	2,6,13,15,17,18	2^{-23}

Table 0.818 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	3,7,18	2,6,11,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	3,7,16,17	2,6,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	3,7	2,6,11,15	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	3,7,16,17,18	2,6,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	3,7,14,17	2,6,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,7,14,16,18	2,6,11,18	2^{-34}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	3,7,14,17,18	2,6,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	3,7,14,16	2,6,11,15	2^{-34}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	3,7	2,6,11,13	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	3,7,16,17,18	2,6,11,13,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	3,7,18	2,6,11,13,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	3,7,16,17	2,6,11,13,15,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,7,14,17,18	2,6,11,13,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	3,7,14,16	2,6,11,13	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	3,7,14,17	2,6,11,13,15,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	3,7,14,16,18	2,6,11,13,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	3,7,12,17	2,6,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	3,7,12,16,18	2,6,11,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	3,7,12,17,18	2,6,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	3,7,12,16	2,6,11,15	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	3,7,12,14,18	2,6,11,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	3,7,12,14,16,17	2,6,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,7,12,14	2,6,11,15	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,7,12,14,16,17,18	2,6,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	3,7,12,17,18	2,6,11,13,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	3,7,12,16	2,6,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	3,7,12,17	2,6,11,13,15,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	3,7,12,16,18	2,6,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	3,7,12,14	2,6,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	3,7,12,14,16,17,18	2,6,11,13,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	3,7,12,14,18	2,6,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	3,7,12,14,16,17	2,6,11,13,15,17	2^{-23}

Table 0.819 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	3,7,10,17,18	2,6,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	3,7,10,16	2,6	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	3,7,10,17	2,6,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	3,7,10,16,18	2,6,15,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	3,7,10,14	2,6	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	3,7,10,14,16,17,18	2,6,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	3,7,10,14,18	2,6,15,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	3,7,10,14,16,17	2,6,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	3,7,10,17	2,6,13,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	3,7,10,16,18	2,6,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	3,7,10,17,18	2,6,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	3,7,10,16	2,6,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	3,7,10,14,18	2,6,13,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	3,7,10,14,16,17	2,6,13,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	3,7,10,14	2,6,13,15	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	3,7,10,14,16,17,18	2,6,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	3,7,10,12	2,6	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	3,7,10,12,16,17,18	2,6,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	3,7,10,12,18	2,6,15,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	3,7,10,12,16,17	2,6,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	3,7,10,12,14,17,18	2,6,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	3,7,10,12,14,16	2,6	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	3,7,10,12,14,17	2,6,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	3,7,10,12,14,16,18	2,6,15,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,7,10,12,18	2,6,13,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	3,7,10,12,16,17	2,6,13,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	3,7,10,12	2,6,13,15	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	3,7,10,12,16,17,18	2,6,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	3,7,10,12,14,17	2,6,13,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	3,7,10,12,14,16,18	2,6,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	3,7,10,12,14,17,18	2,6,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	3,7,10,12,14,16	2,6,13,15	$2^{-17.5}$

Table 0.820 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	3,7,10,17	2,6,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	3,7,10,16,18	2,6,11,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	3,7,10,17,18	2,6,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	3,7,10,16	2,6,11,15	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	3,7,10,14,18	2,6,11,18	2^{-1}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	3,7,10,14,16,17	2,6,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	3,7,10,14	2,6,11,15	2^{-1}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	3,7,10,14,16,17,18	2,6,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,7,10,17,18	2,6,11,13,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	3,7,10,16	2,6,11,13	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	3,7,10,17	2,6,11,13,15,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	3,7,10,16,18	2,6,11,13,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	3,7,10,14	2,6,11,13	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	3,7,10,14,16,17,18	2,6,11,13,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	3,7,10,14,18	2,6,11,13,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	3,7,10,14,16,17	2,6,11,13,15,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	3,7,10,12,18	2,6,11,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	3,7,10,12,16,17	2,6,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	3,7,10,12	2,6,11,15	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	3,7,10,12,16,17,18	2,6,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	3,7,10,12,14,17	2,6,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	3,7,10,12,14,16,18	2,6,11,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	3,7,10,12,14,17,18	2,6,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	3,7,10,12,14,16	2,6,11,15	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	3,7,10,12	2,6,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	3,7,10,12,16,17,18	2,6,11,13,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	3,7,10,12,18	2,6,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	3,7,10,12,16,17	2,6,11,13,15,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	3,7,10,12,14,17,18	2,6,11,13,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	3,7,10,12,14,16	2,6,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	3,7,10,12,14,17	2,6,11,13,15,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	3,7,10,12,14,16,18	2,6,11,13,15,18	$2^{-17.5}$

Table 0.821 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,7,18	2,6,9,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	3,7,16,17	2,6,9,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	3,7	2,6,9,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	3,7,16,17,18	2,6,9,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	3,7,14,17	2,6,9,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	3,7,14,16,18	2,6,9,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	3,7,14,17,18	2,6,9,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	3,7,14,16	2,6,9,15	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	3,7	2,6,9,13	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	3,7,16,17,18	2,6,9,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	3,7,18	2,6,9,13,15,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	3,7,16,17	2,6,9,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	3,7,14,17,18	2,6,9,13,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	3,7,14,16	2,6,9,13	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	3,7,14,17	2,6,9,13,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	3,7,14,16,18	2,6,9,13,15,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	3,7,12,17	2,6,9,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	3,7,12,16,18	2,6,9,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	3,7,12,17,18	2,6,9,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	3,7,12,16	2,6,9,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	3,7,12,14,18	2,6,9,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	3,7,12,14,16,17	2,6,9,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	3,7,12,14	2,6,9,15	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	3,7,12,14,16,17,18	2,6,9,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	3,7,12,17,18	2,6,9,13,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	3,7,12,16	2,6,9,13	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	3,7,12,17	2,6,9,13,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	3,7,12,16,18	2,6,9,13,15,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	3,7,12,14	2,6,9,13	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	3,7,12,14,16,17,18	2,6,9,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	3,7,12,14,18	2,6,9,13,15,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	3,7,12,14,16,17	2,6,9,13,15,17	$2^{-17.5}$

Table 0.822 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	3,7	2,6,9,11	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	3,7,16,17,18	2,6,9,11,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	3,7,18	2,6,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	3,7,16,17	2,6,9,11,15,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	3,7,14,17,18	2,6,9,11,17,18	2^{-1}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	3,7,14,16	2,6,9,11	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	3,7,14,17	2,6,9,11,15,17	2^{-1}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	3,7,14,16,18	2,6,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,7,18	2,6,9,11,13,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,7,16,17	2,6,9,11,13,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	3,7	2,6,9,11,13,15	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	3,7,16,17,18	2,6,9,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	3,7,14,17	2,6,9,11,13,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	3,7,14,16,18	2,6,9,11,13,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	3,7,14,17,18	2,6,9,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	3,7,14,16	2,6,9,11,13,15	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	3,7,12,17,18	2,6,9,11,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	3,7,12,16	2,6,9,11	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,7,12,17	2,6,9,11,15,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	3,7,12,16,18	2,6,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	3,7,12,14	2,6,9,11	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	3,7,12,14,16,17,18	2,6,9,11,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	3,7,12,14,18	2,6,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	3,7,12,14,16,17	2,6,9,11,15,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	3,7,12,17	2,6,9,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	3,7,12,16,18	2,6,9,11,13,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	3,7,12,17,18	2,6,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	3,7,12,16	2,6,9,11,13,15	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	3,7,12,14,18	2,6,9,11,13,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	3,7,12,14,16,17	2,6,9,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	3,7,12,14	2,6,9,11,13,15	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	3,7,12,14,16,17,18	2,6,9,11,13,15,17,18	$2^{-17.5}$

Table 0.823 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	3,7,10,17	2,6,9,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	3,7,10,16,18	2,6,9,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	3,7,10,17,18	2,6,9,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	3,7,10,16	2,6,9,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	3,7,10,14,18	2,6,9,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	3,7,10,14,16,17	2,6,9,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	3,7,10,14	2,6,9,15	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	3,7,10,14,16,17,18	2,6,9,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	3,7,10,17,18	2,6,9,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	3,7,10,16	2,6,9,13	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	3,7,10,17	2,6,9,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	3,7,10,16,18	2,6,9,13,15,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	3,7,10,14	2,6,9,13	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	3,7,10,14,16,17,18	2,6,9,13,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	3,7,10,14,18	2,6,9,13,15,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	3,7,10,14,16,17	2,6,9,13,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	3,7,10,12,18	2,6,9,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	3,7,10,12,16,17	2,6,9,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	3,7,10,12	2,6,9,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	3,7,10,12,16,17,18	2,6,9,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	3,7,10,12,14,17	2,6,9,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	3,7,10,12,14,16,18	2,6,9,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	3,7,10,12,14,17,18	2,6,9,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	3,7,10,12,14,16	2,6,9,15	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	3,7,10,12	2,6,9,13	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	3,7,10,12,16,17,18	2,6,9,13,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	3,7,10,12,18	2,6,9,13,15,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	3,7,10,12,16,17	2,6,9,13,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	3,7,10,12,14,17,18	2,6,9,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	3,7,10,12,14,16	2,6,9,13	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	3,7,10,12,14,17	2,6,9,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	3,7,10,12,14,16,18	2,6,9,13,15,18	2^{-23}

Table 0.824 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	3,7,10,17,18	2,6,9,11,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	3,7,10,16	2,6,9,11	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,7,10,17	2,6,9,11,15,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	3,7,10,16,18	2,6,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	3,7,10,14	2,6,9,11	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	3,7,10,14,16,17,18	2,6,9,11,17,18	2^{-34}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	3,7,10,14,18	2,6,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	3,7,10,14,16,17	2,6,9,11,15,17	2^{-34}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	3,7,10,17	2,6,9,11,13,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	3,7,10,16,18	2,6,9,11,13,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	3,7,10,17,18	2,6,9,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	3,7,10,16	2,6,9,11,13,15	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	3,7,10,14,18	2,6,9,11,13,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	3,7,10,14,16,17	2,6,9,11,13,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	3,7,10,14	2,6,9,11,13,15	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	3,7,10,14,16,17,18	2,6,9,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	3,7,10,12	2,6,9,11	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,7,10,12,16,17,18	2,6,9,11,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	3,7,10,12,18	2,6,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	3,7,10,12,16,17	2,6,9,11,15,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	3,7,10,12,14,17,18	2,6,9,11,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	3,7,10,12,14,16	2,6,9,11	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	3,7,10,12,14,17	2,6,9,11,15,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	3,7,10,12,14,16,18	2,6,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	3,7,10,12,18	2,6,9,11,13,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,7,10,12,16,17	2,6,9,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	3,7,10,12	2,6,9,11,13,15	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	3,7,10,12,16,17,18	2,6,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	3,7,10,12,14,17	2,6,9,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	3,7,10,12,14,16,18	2,6,9,11,13,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	3,7,10,12,14,17,18	2,6,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	3,7,10,12,14,16	2,6,9,11,13,15	2^{-23}

Table 0.825 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	3,7,17,18	2,6,8,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	3,7,16	2,6,8	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	3,7,17	2,6,8,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	3,7,16,18	2,6,8,15,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	3,7,14	2,6,8	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	3,7,14,16,17,18	2,6,8,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	3,7,14,18	2,6,8,15,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	3,7,14,16,17	2,6,8,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	3,7,17	2,6,8,13,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	3,7,16,18	2,6,8,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	3,7,17,18	2,6,8,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	3,7,16	2,6,8,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	3,7,14,18	2,6,8,13,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	3,7,14,16,17	2,6,8,13,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	3,7,14	2,6,8,13,15	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	3,7,14,16,17,18	2,6,8,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	3,7,12	2,6,8	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	3,7,12,16,17,18	2,6,8,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	3,7,12,18	2,6,8,15,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	3,7,12,16,17	2,6,8,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	3,7,12,14,17,18	2,6,8,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	3,7,12,14,16	2,6,8	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	3,7,12,14,17	2,6,8,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	3,7,12,14,16,18	2,6,8,15,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	3,7,12,18	2,6,8,13,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	3,7,12,16,17	2,6,8,13,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	3,7,12	2,6,8,13,15	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	3,7,12,16,17,18	2,6,8,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	3,7,12,14,17	2,6,8,13,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	3,7,12,14,16,18	2,6,8,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	3,7,12,14,17,18	2,6,8,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	3,7,12,14,16	2,6,8,13,15	$2^{-17.5}$

Table 0.826 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	3,7,17	2,6,8,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	3,7,16,18	2,6,8,11,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	3,7,17,18	2,6,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,7,16	2,6,8,11,15	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	3,7,14,18	2,6,8,11,18	2^{-34}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	3,7,14,16,17	2,6,8,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	3,7,14	2,6,8,11,15	2^{-34}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	3,7,14,16,17,18	2,6,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	3,7,17,18	2,6,8,11,13,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	3,7,16	2,6,8,11,13	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	3,7,17	2,6,8,11,13,15,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	3,7,16,18	2,6,8,11,13,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	3,7,14	2,6,8,11,13	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	3,7,14,16,17,18	2,6,8,11,13,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	3,7,14,18	2,6,8,11,13,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	3,7,14,16,17	2,6,8,11,13,15,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,7,12,18	2,6,8,11,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	3,7,12,16,17	2,6,8,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	3,7,12	2,6,8,11,15	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	3,7,12,16,17,18	2,6,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	3,7,12,14,17	2,6,8,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	3,7,12,14,16,18	2,6,8,11,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	3,7,12,14,17,18	2,6,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	3,7,12,14,16	2,6,8,11,15	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,7,12	2,6,8,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	3,7,12,16,17,18	2,6,8,11,13,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	3,7,12,18	2,6,8,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	3,7,12,16,17	2,6,8,11,13,15,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,7,12,14,17,18	2,6,8,11,13,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	3,7,12,14,16	2,6,8,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	3,7,12,14,17	2,6,8,11,13,15,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	3,7,12,14,16,18	2,6,8,11,13,15,18	$2^{-17.5}$

Table 0.827 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	3,7,10	2,6,8	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,7,10,16,17,18	2,6,8,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	3,7,10,18	2,6,8,15,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	3,7,10,16,17	2,6,8,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	3,7,10,14,17,18	2,6,8,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	3,7,10,14,16	2,6,8	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	3,7,10,14,17	2,6,8,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	3,7,10,14,16,18	2,6,8,15,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	3,7,10,18	2,6,8,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	3,7,10,16,17	2,6,8,13,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	3,7,10	2,6,8,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	3,7,10,16,17,18	2,6,8,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	3,7,10,14,17	2,6,8,13,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	3,7,10,14,16,18	2,6,8,13,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	3,7,10,14,17,18	2,6,8,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	3,7,10,14,16	2,6,8,13,15	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	3,7,10,12,17,18	2,6,8,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	3,7,10,12,16	2,6,8	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	3,7,10,12,17	2,6,8,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	3,7,10,12,16,18	2,6,8,15,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	3,7,10,12,14	2,6,8	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	3,7,10,12,14,16,17,18	2,6,8,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	3,7,10,12,14,18	2,6,8,15,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	3,7,10,12,14,16,17	2,6,8,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	3,7,10,12,17	2,6,8,13,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	3,7,10,12,16,18	2,6,8,13,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	3,7,10,12,17,18	2,6,8,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	3,7,10,12,16	2,6,8,13,15	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	3,7,10,12,14,18	2,6,8,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	3,7,10,12,14,16,17	2,6,8,13,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	3,7,10,12,14	2,6,8,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	3,7,10,12,14,16,17,18	2,6,8,13,15,17,18	2^{-12}

Table 0.828 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	3,7,10,18	2,6,8,11,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	3,7,10,16,17	2,6,8,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	3,7,10	2,6,8,11,15	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	3,7,10,16,17,18	2,6,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	3,7,10,14,17	2,6,8,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	3,7,10,14,16,18	2,6,8,11,18	2^{-1}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	3,7,10,14,17,18	2,6,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	3,7,10,14,16	2,6,8,11,15	2^{-1}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,7,10	2,6,8,11,13	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,7,10,16,17,18	2,6,8,11,13,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	3,7,10,18	2,6,8,11,13,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	3,7,10,16,17	2,6,8,11,13,15,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	3,7,10,14,17,18	2,6,8,11,13,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	3,7,10,14,16	2,6,8,11,13	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	3,7,10,14,17	2,6,8,11,13,15,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	3,7,10,14,16,18	2,6,8,11,13,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	3,7,10,12,17	2,6,8,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	3,7,10,12,16,18	2,6,8,11,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	3,7,10,12,17,18	2,6,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,7,10,12,16	2,6,8,11,15	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	3,7,10,12,14,18	2,6,8,11,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	3,7,10,12,14,16,17	2,6,8,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	3,7,10,12,14	2,6,8,11,15	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	3,7,10,12,14,16,17,18	2,6,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	3,7,10,12,17,18	2,6,8,11,13,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	3,7,10,12,16	2,6,8,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	3,7,10,12,17	2,6,8,11,13,15,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	3,7,10,12,16,18	2,6,8,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	3,7,10,12,14	2,6,8,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	3,7,10,12,14,16,17,18	2,6,8,11,13,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	3,7,10,12,14,18	2,6,8,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	3,7,10,12,14,16,17	2,6,8,11,13,15,17	2^{-12}

Table 0.829 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	3,7,17	2,6,8,9,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	3,7,16,18	2,6,8,9,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	3,7,17,18	2,6,8,9,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	3,7,16	2,6,8,9,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	3,7,14,18	2,6,8,9,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	3,7,14,16,17	2,6,8,9,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	3,7,14	2,6,8,9,15	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	3,7,14,16,17,18	2,6,8,9,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	3,7,17,18	2,6,8,9,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,7,16	2,6,8,9,13	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	3,7,17	2,6,8,9,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	3,7,16,18	2,6,8,9,13,15,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	3,7,14	2,6,8,9,13	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	3,7,14,16,17,18	2,6,8,9,13,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	3,7,14,18	2,6,8,9,13,15,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	3,7,14,16,17	2,6,8,9,13,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	3,7,12,18	2,6,8,9,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	3,7,12,16,17	2,6,8,9,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	3,7,12	2,6,8,9,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	3,7,12,16,17,18	2,6,8,9,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	3,7,12,14,17	2,6,8,9,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	3,7,12,14,16,18	2,6,8,9,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	3,7,12,14,17,18	2,6,8,9,15,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	3,7,12,14,16	2,6,8,9,15	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	3,7,12	2,6,8,9,13	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,7,12,16,17,18	2,6,8,9,13,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	3,7,12,18	2,6,8,9,13,15,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,7,12,16,17	2,6,8,9,13,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	3,7,12,14,17,18	2,6,8,9,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	3,7,12,14,16	2,6,8,9,13	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	3,7,12,14,17	2,6,8,9,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	3,7,12,14,16,18	2,6,8,9,13,15,18	2^{-12}

Table 0.830 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	3,7,17,18	2,6,8,9,11,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	3,7,16	2,6,8,9,11	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	3,7,17	2,6,8,9,11,15,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	3,7,16,18	2,6,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	3,7,14	2,6,8,9,11	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	3,7,14,16,17,18	2,6,8,9,11,17,18	2^{-1}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	3,7,14,18	2,6,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	3,7,14,16,17	2,6,8,9,11,15,17	2^{-1}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	3,7,17	2,6,8,9,11,13,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,7,16,18	2,6,8,9,11,13,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	3,7,17,18	2,6,8,9,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	3,7,16	2,6,8,9,11,13,15	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	3,7,14,18	2,6,8,9,11,13,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	3,7,14,16,17	2,6,8,9,11,13,17	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	3,7,14	2,6,8,9,11,13,15	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	3,7,14,16,17,18	2,6,8,9,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	3,7,12	2,6,8,9,11	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	3,7,12,16,17,18	2,6,8,9,11,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	3,7,12,18	2,6,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	3,7,12,16,17	2,6,8,9,11,15,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	3,7,12,14,17,18	2,6,8,9,11,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	3,7,12,14,16	2,6,8,9,11	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	3,7,12,14,17	2,6,8,9,11,15,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	3,7,12,14,16,18	2,6,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	3,7,12,18	2,6,8,9,11,13,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	3,7,12,16,17	2,6,8,9,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	3,7,12	2,6,8,9,11,13,15	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	3,7,12,16,17,18	2,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	3,7,12,14,17	2,6,8,9,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	3,7,12,14,16,18	2,6,8,9,11,13,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	3,7,12,14,17,18	2,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	3,7,12,14,16	2,6,8,9,11,13,15	2^{-12}

Table 0.831 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	3,7,10,18	2,6,8,9,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	3,7,10,16,17	2,6,8,9,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	3,7,10	2,6,8,9,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	3,7,10,16,17,18	2,6,8,9,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	3,7,10,14,17	2,6,8,9,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	3,7,10,14,16,18	2,6,8,9,18	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	3,7,10,14,17,18	2,6,8,9,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,7,10,14,16	2,6,8,9,15	$2^{-6.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	3,7,10	2,6,8,9,13	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	3,7,10,16,17,18	2,6,8,9,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	3,7,10,18	2,6,8,9,13,15,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	3,7,10,16,17	2,6,8,9,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	3,7,10,14,17,18	2,6,8,9,13,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	3,7,10,14,16	2,6,8,9,13	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	3,7,10,14,17	2,6,8,9,13,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	3,7,10,14,16,18	2,6,8,9,13,15,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	3,7,10,12,17	2,6,8,9,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,7,10,12,16,18	2,6,8,9,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	3,7,10,12,17,18	2,6,8,9,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	3,7,10,12,16	2,6,8,9,15	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	3,7,10,12,14,18	2,6,8,9,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	3,7,10,12,14,16,17	2,6,8,9,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	3,7,10,12,14	2,6,8,9,15	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	3,7,10,12,14,16,17,18	2,6,8,9,15,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	3,7,10,12,17,18	2,6,8,9,13,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,7,10,12,16	2,6,8,9,13	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	3,7,10,12,17	2,6,8,9,13,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	3,7,10,12,16,18	2,6,8,9,13,15,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	3,7,10,12,14	2,6,8,9,13	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	3,7,10,12,14,16,17,18	2,6,8,9,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	3,7,10,12,14,18	2,6,8,9,13,15,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	3,7,10,12,14,16,17	2,6,8,9,13,15,17	$2^{-17.5}$

Table 0.832 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	3,7,10	2,6,8,9,11	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	3,7,10,16,17,18	2,6,8,9,11,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	3,7,10,18	2,6,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	3,7,10,16,17	2,6,8,9,11,15,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	3,7,10,14,17,18	2,6,8,9,11,17,18	2^{-34}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	3,7,10,14,16	2,6,8,9,11	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	3,7,10,14,17	2,6,8,9,11,15,17	2^{-34}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	3,7,10,14,16,18	2,6,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	3,7,10,18	2,6,8,9,11,13,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	3,7,10,16,17	2,6,8,9,11,13,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	3,7,10	2,6,8,9,11,13,15	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	3,7,10,16,17,18	2,6,8,9,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	3,7,10,14,17	2,6,8,9,11,13,17	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,7,10,14,16,18	2,6,8,9,11,13,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	3,7,10,14,17,18	2,6,8,9,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	3,7,10,14,16	2,6,8,9,11,13,15	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	3,7,10,12,17,18	2,6,8,9,11,17,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	3,7,10,12,16	2,6,8,9,11	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	3,7,10,12,17	2,6,8,9,11,15,17	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	3,7,10,12,16,18	2,6,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	3,7,10,12,14	2,6,8,9,11	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	3,7,10,12,14,16,17,18	2,6,8,9,11,17,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,7,10,12,14,18	2,6,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,7,10,12,14,16,17	2,6,8,9,11,15,17	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	3,7,10,12,17	2,6,8,9,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	3,7,10,12,16,18	2,6,8,9,11,13,18	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	3,7,10,12,17,18	2,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	3,7,10,12,16	2,6,8,9,11,13,15	2^{-12}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	3,7,10,12,14,18	2,6,8,9,11,13,18	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	3,7,10,12,14,16,17	2,6,8,9,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	3,7,10,12,14	2,6,8,9,11,13,15	2^{-23}
$(0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	3,7,10,12,14,16,17,18	2,6,8,9,11,13,15,17,18	$2^{-17.5}$

Table 0.833 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	3,5,17,18	2,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	3,5,16	2	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	3,5,17	2,15,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	3,5,16,18	2,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	3,5,14	2	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	3,5,14,16,17,18	2,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	3,5,14,18	2,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	3,5,14,16,17	2,15,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	3,5,17	2,13,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	3,5,16,18	2,13,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,17,18	2,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	3,5,16	2,13,15	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	3,5,14,18	2,13,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,14,16,17	2,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	3,5,14	2,13,15	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,14,16,17,18	2,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,12	2	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	3,5,12,16,17,18	2,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,12,18	2,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	3,5,12,16,17	2,15,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	3,5,12,14,17,18	2,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	3,5,12,14,16	2	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	3,5,12,14,17	2,15,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	3,5,12,14,16,18	2,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	3,5,12,18	2,13,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	3,5,12,16,17	2,13,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	3,5,12	2,13,15	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	3,5,12,16,17,18	2,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	3,5,12,14,17	2,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,12,14,16,18	2,13,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	3,5,12,14,17,18	2,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,12,14,16	2,13,15	2^{-23}

Table 0.834 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	3,5,17	2,11,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	3,5,16,18	2,11,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	3,5,17,18	2,11,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	3,5,16	2,11,15	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	3,5,14,18	2,11,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	3,5,14,16,17	2,11,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	3,5,14	2,11,15	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,5,14,16,17,18	2,11,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	3,5,17,18	2,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	3,5,16	2,11,13	2^{-34}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	3,5,17	2,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	3,5,16,18	2,11,13,15,18	2^{-34}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	3,5,14	2,11,13	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	3,5,14,16,17,18	2,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	3,5,14,18	2,11,13,15,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,5,14,16,17	2,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	3,5,12,18	2,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	3,5,12,16,17	2,11,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	3,5,12	2,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	3,5,12,16,17,18	2,11,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,5,12,14,17	2,11,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	3,5,12,14,16,18	2,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	3,5,12,14,17,18	2,11,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	3,5,12,14,16	2,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	3,5,12	2,11,13	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	3,5,12,16,17,18	2,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	3,5,12,18	2,11,13,15,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	3,5,12,16,17	2,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	3,5,12,14,17,18	2,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	3,5,12,14,16	2,11,13	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	3,5,12,14,17	2,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	3,5,12,14,16,18	2,11,13,15,18	2^{-23}

Table 0.835 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	3,5,10	2	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	3,5,10,16,17,18	2,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	3,5,10,18	2,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	3,5,10,16,17	2,15,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	3,5,10,14,17,18	2,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	3,5,10,14,16	2	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	3,5,10,14,17	2,15,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	3,5,10,14,16,18	2,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	3,5,10,18	2,13,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	3,5,10,16,17	2,13,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	3,5,10	2,13,15	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	3,5,10,16,17,18	2,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	3,5,10,14,17	2,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	3,5,10,14,16,18	2,13,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	3,5,10,14,17,18	2,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	3,5,10,14,16	2,13,15	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	3,5,10,12,17,18	2,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	3,5,10,12,16	2	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	3,5,10,12,17	2,15,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	3,5,10,12,16,18	2,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5,10,12,14	2	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	3,5,10,12,14,16,17,18	2,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5,10,12,14,18	2,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,10,12,14,16,17	2,15,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,10,12,17	2,13,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	3,5,10,12,16,18	2,13,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,10,12,17,18	2,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	3,5,10,12,16	2,13,15	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	3,5,10,12,14,18	2,13,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	3,5,10,12,14,16,17	2,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	3,5,10,12,14	2,13,15	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	3,5,10,12,14,16,17,18	2,13,15,17,18	$2^{-17.5}$

Table 0.836 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	3,5,10,18	2,11,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	3,5,10,16,17	2,11,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	3,5,10	2,11,15	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	3,5,10,16,17,18	2,11,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,5,10,14,17	2,11,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	3,5,10,14,16,18	2,11,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	3,5,10,14,17,18	2,11,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	3,5,10,14,16	2,11,15	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	3,5,10	2,11,13	2^{-1}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	3,5,10,16,17,18	2,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	3,5,10,18	2,11,13,15,18	2^{-1}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	3,5,10,16,17	2,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	3,5,10,14,17,18	2,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	3,5,10,14,16	2,11,13	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	3,5,10,14,17	2,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	3,5,10,14,16,18	2,11,13,15,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	3,5,10,12,17	2,11,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	3,5,10,12,16,18	2,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	3,5,10,12,17,18	2,11,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	3,5,10,12,16	2,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	3,5,10,12,14,18	2,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	3,5,10,12,14,16,17	2,11,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	3,5,10,12,14	2,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	3,5,10,12,14,16,17,18	2,11,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	3,5,10,12,17,18	2,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	3,5,10,12,16	2,11,13	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	3,5,10,12,17	2,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	3,5,10,12,16,18	2,11,13,15,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	3,5,10,12,14	2,11,13	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,10,12,14,16,17,18	2,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	3,5,10,12,14,18	2,11,13,15,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,10,12,14,16,17	2,11,13,15,17	$2^{-17.5}$

Table 0.837 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	3,5,17	2,9,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	3,5,16,18	2,9,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	3,5,17,18	2,9,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	3,5,16	2,9,15	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	3,5,14,18	2,9,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	3,5,14,16,17	2,9,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	3,5,14	2,9,15	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	3,5,14,16,17,18	2,9,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	3,5,17,18	2,9,13,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	3,5,16	2,9,13	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	3,5,17	2,9,13,15,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	3,5,16,18	2,9,13,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	3,5,14	2,9,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	3,5,14,16,17,18	2,9,13,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,5,14,18	2,9,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	3,5,14,16,17	2,9,13,15,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	3,5,12,18	2,9,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	3,5,12,16,17	2,9,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	3,5,12	2,9,15	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	3,5,12,16,17,18	2,9,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	3,5,12,14,17	2,9,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	3,5,12,14,16,18	2,9,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	3,5,12,14,17,18	2,9,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	3,5,12,14,16	2,9,15	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	3,5,12	2,9,13	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	3,5,12,16,17,18	2,9,13,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	3,5,12,18	2,9,13,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	3,5,12,16,17	2,9,13,15,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	3,5,12,14,17,18	2,9,13,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	3,5,12,14,16	2,9,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	3,5,12,14,17	2,9,13,15,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	3,5,12,14,16,18	2,9,13,15,18	$2^{-17.5}$

Table 0.838 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	3,5,17,18	2,9,11,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	3,5,16	2,9,11	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	3,5,17	2,9,11,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	3,5,16,18	2,9,11,15,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	3,5,14	2,9,11	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,14,16,17,18	2,9,11,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	3,5,14,18	2,9,11,15,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,14,16,17	2,9,11,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	3,5,17	2,9,11,13,17	2^{-1}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	3,5,16,18	2,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	3,5,17,18	2,9,11,13,15,17,18	2^{-1}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	3,5,16	2,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	3,5,14,18	2,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	3,5,14,16,17	2,9,11,13,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	3,5,14	2,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	3,5,14,16,17,18	2,9,11,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5,12	2,9,11	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	3,5,12,16,17,18	2,9,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	3,5,12,18	2,9,11,15,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	3,5,12,16,17	2,9,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	3,5,12,14,17,18	2,9,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	3,5,12,14,16	2,9,11	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	3,5,12,14,17	2,9,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	3,5,12,14,16,18	2,9,11,15,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	3,5,12,18	2,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	3,5,12,16,17	2,9,11,13,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	3,5,12	2,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	3,5,12,16,17,18	2,9,11,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	3,5,12,14,17	2,9,11,13,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	3,5,12,14,16,18	2,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	3,5,12,14,17,18	2,9,11,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	3,5,12,14,16	2,9,11,13,15	$2^{-17.5}$

Table 0.839 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	3,5,10,18	2,9,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	3,5,10,16,17	2,9,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	3,5,10	2,9,15	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	3,5,10,16,17,18	2,9,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	3,5,10,14,17	2,9,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	3,5,10,14,16,18	2,9,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,5,10,14,17,18	2,9,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	3,5,10,14,16	2,9,15	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	3,5,10	2,9,13	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	3,5,10,16,17,18	2,9,13,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	3,5,10,18	2,9,13,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	3,5,10,16,17	2,9,13,15,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,10,14,17,18	2,9,13,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	3,5,10,14,16	2,9,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,10,14,17	2,9,13,15,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	3,5,10,14,16,18	2,9,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,5,10,12,17	2,9,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	3,5,10,12,16,18	2,9,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	3,5,10,12,17,18	2,9,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	3,5,10,12,16	2,9,15	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	3,5,10,12,14,18	2,9,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	3,5,10,12,14,16,17	2,9,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	3,5,10,12,14	2,9,15	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	3,5,10,12,14,16,17,18	2,9,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	3,5,10,12,17,18	2,9,13,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	3,5,10,12,16	2,9,13	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	3,5,10,12,17	2,9,13,15,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	3,5,10,12,16,18	2,9,13,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	3,5,10,12,14	2,9,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	3,5,10,12,14,16,17,18	2,9,13,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	3,5,10,12,14,18	2,9,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	3,5,10,12,14,16,17	2,9,13,15,17	2^{-23}

Table 0.840 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,5,10	2,9,11	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,5,10,16,17,18	2,9,11,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	3,5,10,18	2,9,11,15,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	3,5,10,16,17	2,9,11,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	3,5,10,14,17,18	2,9,11,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	3,5,10,14,16	2,9,11	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	3,5,10,14,17	2,9,11,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	3,5,10,14,16,18	2,9,11,15,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	3,5,10,18	2,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	3,5,10,16,17	2,9,11,13,17	2^{-34}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	3,5,10	2,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	3,5,10,16,17,18	2,9,11,13,15,17,18	2^{-34}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	3,5,10,14,17	2,9,11,13,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	3,5,10,14,16,18	2,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	3,5,10,14,17,18	2,9,11,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	3,5,10,14,16	2,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	3,5,10,12,17,18	2,9,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	3,5,10,12,16	2,9,11	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	3,5,10,12,17	2,9,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	3,5,10,12,16,18	2,9,11,15,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	3,5,10,12,14	2,9,11	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	3,5,10,12,14,16,17,18	2,9,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	3,5,10,12,14,18	2,9,11,15,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	3,5,10,12,14,16,17	2,9,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,10,12,17	2,9,11,13,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	3,5,10,12,16,18	2,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,10,12,17,18	2,9,11,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	3,5,10,12,16	2,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	3,5,10,12,14,18	2,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	3,5,10,12,14,16,17	2,9,11,13,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	3,5,10,12,14	2,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	3,5,10,12,14,16,17,18	2,9,11,13,15,17,18	2^{-23}

Table 0.841 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	3,5	2,8	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	3,5,16,17,18	2,8,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	3,5,18	2,8,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	3,5,16,17	2,8,15,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	3,5,14,17,18	2,8,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	3,5,14,16	2,8	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	3,5,14,17	2,8,15,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,5,14,16,18	2,8,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	3,5,18	2,8,13,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	3,5,16,17	2,8,13,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	3,5	2,8,13,15	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	3,5,16,17,18	2,8,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	3,5,14,17	2,8,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,14,16,18	2,8,13,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	3,5,14,17,18	2,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,14,16	2,8,13,15	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	3,5,12,17,18	2,8,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,5,12,16	2,8	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	3,5,12,17	2,8,15,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	3,5,12,16,18	2,8,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	3,5,12,14	2,8	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	3,5,12,14,16,17,18	2,8,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	3,5,12,14,18	2,8,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	3,5,12,14,16,17	2,8,15,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	3,5,12,17	2,8,13,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	3,5,12,16,18	2,8,13,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	3,5,12,17,18	2,8,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	3,5,12,16	2,8,13,15	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	3,5,12,14,18	2,8,13,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	3,5,12,14,16,17	2,8,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	3,5,12,14	2,8,13,15	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	3,5,12,14,16,17,18	2,8,13,15,17,18	$2^{-17.5}$

Table 0.842 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,5,18	2,8,11,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,5,16,17	2,8,11,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	3,5	2,8,11,15	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	3,5,16,17,18	2,8,11,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	3,5,14,17	2,8,11,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	3,5,14,16,18	2,8,11,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	3,5,14,17,18	2,8,11,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	3,5,14,16	2,8,11,15	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	3,5	2,8,11,13	2^{-34}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	3,5,16,17,18	2,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	3,5,18	2,8,11,13,15,18	2^{-34}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	3,5,16,17	2,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	3,5,14,17,18	2,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	3,5,14,16	2,8,11,13	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	3,5,14,17	2,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	3,5,14,16,18	2,8,11,13,15,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	3,5,12,17	2,8,11,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	3,5,12,16,18	2,8,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	3,5,12,17,18	2,8,11,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	3,5,12,16	2,8,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	3,5,12,14,18	2,8,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,12,14,16,17	2,8,11,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	3,5,12,14	2,8,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	3,5,12,14,16,17,18	2,8,11,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	3,5,12,17,18	2,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,12,16	2,8,11,13	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	3,5,12,17	2,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,12,16,18	2,8,11,13,15,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	3,5,12,14	2,8,11,13	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	3,5,12,14,16,17,18	2,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	3,5,12,14,18	2,8,11,13,15,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	3,5,12,14,16,17	2,8,11,13,15,17	$2^{-17.5}$

Table 0.843 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	3,5,10,17,18	2,8,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	3,5,10,16	2,8	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	3,5,10,17	2,8,15,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	3,5,10,16,18	2,8,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	3,5,10,14	2,8	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	3,5,10,14,16,17,18	2,8,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	3,5,10,14,18	2,8,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	3,5,10,14,16,17	2,8,15,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	3,5,10,17	2,8,13,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	3,5,10,16,18	2,8,13,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	3,5,10,17,18	2,8,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	3,5,10,16	2,8,13,15	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	3,5,10,14,18	2,8,13,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	3,5,10,14,16,17	2,8,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	3,5,10,14	2,8,13,15	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,5,10,14,16,17,18	2,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	3,5,10,12	2,8	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	3,5,10,12,16,17,18	2,8,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	3,5,10,12,18	2,8,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	3,5,10,12,16,17	2,8,15,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	3,5,10,12,14,17,18	2,8,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	3,5,10,12,14,16	2,8	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	3,5,10,12,14,17	2,8,15,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	3,5,10,12,14,16,18	2,8,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	3,5,10,12,18	2,8,13,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	3,5,10,12,16,17	2,8,13,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	3,5,10,12	2,8,13,15	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	3,5,10,12,16,17,18	2,8,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	3,5,10,12,14,17	2,8,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	3,5,10,12,14,16,18	2,8,13,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	3,5,10,12,14,17,18	2,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	3,5,10,12,14,16	2,8,13,15	2^{-12}

Table 0.844 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,10,17	2,8,11,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	3,5,10,16,18	2,8,11,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	3,5,10,17,18	2,8,11,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	3,5,10,16	2,8,11,15	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	3,5,10,14,18	2,8,11,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	3,5,10,14,16,17	2,8,11,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	3,5,10,14	2,8,11,15	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	3,5,10,14,16,17,18	2,8,11,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	3,5,10,17,18	2,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	3,5,10,16	2,8,11,13	2^{-1}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	3,5,10,17	2,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	3,5,10,16,18	2,8,11,13,15,18	2^{-1}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	3,5,10,14	2,8,11,13	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	3,5,10,14,16,17,18	2,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	3,5,10,14,18	2,8,11,13,15,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	3,5,10,14,16,17	2,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	3,5,10,12,18	2,8,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	3,5,10,12,16,17	2,8,11,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	3,5,10,12	2,8,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	3,5,10,12,16,17,18	2,8,11,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	3,5,10,12,14,17	2,8,11,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	3,5,10,12,14,16,18	2,8,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	3,5,10,12,14,17,18	2,8,11,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	3,5,10,12,14,16	2,8,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	3,5,10,12	2,8,11,13	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	3,5,10,12,16,17,18	2,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	3,5,10,12,18	2,8,11,13,15,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	3,5,10,12,16,17	2,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	3,5,10,12,14,17,18	2,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	3,5,10,12,14,16	2,8,11,13	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	3,5,10,12,14,17	2,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,5,10,12,14,16,18	2,8,11,13,15,18	2^{-12}

Table 0.845 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	3,5,18	2,8,9,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	3,5,16,17	2,8,9,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	3,5	2,8,9,15	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	3,5,16,17,18	2,8,9,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	3,5,14,17	2,8,9,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	3,5,14,16,18	2,8,9,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	3,5,14,17,18	2,8,9,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	3,5,14,16	2,8,9,15	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	3,5	2,8,9,13	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	3,5,16,17,18	2,8,9,13,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	3,5,18	2,8,9,13,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	3,5,16,17	2,8,9,13,15,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	3,5,14,17,18	2,8,9,13,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	3,5,14,16	2,8,9,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	3,5,14,17	2,8,9,13,15,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	3,5,14,16,18	2,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	3,5,12,17	2,8,9,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	3,5,12,16,18	2,8,9,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	3,5,12,17,18	2,8,9,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	3,5,12,16	2,8,9,15	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	3,5,12,14,18	2,8,9,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5,12,14,16,17	2,8,9,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	3,5,12,14	2,8,9,15	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5,12,14,16,17,18	2,8,9,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	3,5,12,17,18	2,8,9,13,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,12,16	2,8,9,13	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	3,5,12,17	2,8,9,13,15,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,12,16,18	2,8,9,13,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	3,5,12,14	2,8,9,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	3,5,12,14,16,17,18	2,8,9,13,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	3,5,12,14,18	2,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	3,5,12,14,16,17	2,8,9,13,15,17	2^{-12}

Table 0.846 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	3,5	2,8,9,11	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	3,5,16,17,18	2,8,9,11,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	3,5,18	2,8,9,11,15,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	3,5,16,17	2,8,9,11,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	3,5,14,17,18	2,8,9,11,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,5,14,16	2,8,9,11	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	3,5,14,17	2,8,9,11,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	3,5,14,16,18	2,8,9,11,15,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	3,5,18	2,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	3,5,16,17	2,8,9,11,13,17	2^{-1}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	3,5	2,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	3,5,16,17,18	2,8,9,11,13,15,17,18	2^{-1}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	3,5,14,17	2,8,9,11,13,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	3,5,14,16,18	2,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	3,5,14,17,18	2,8,9,11,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	3,5,14,16	2,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	3,5,12,17,18	2,8,9,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	3,5,12,16	2,8,9,11	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	3,5,12,17	2,8,9,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	3,5,12,16,18	2,8,9,11,15,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	3,5,12,14	2,8,9,11	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	3,5,12,14,16,17,18	2,8,9,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	3,5,12,14,18	2,8,9,11,15,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	3,5,12,14,16,17	2,8,9,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	3,5,12,17	2,8,9,11,13,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	3,5,12,16,18	2,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	3,5,12,17,18	2,8,9,11,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	3,5,12,16	2,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,12,14,18	2,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	3,5,12,14,16,17	2,8,9,11,13,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,12,14	2,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5,12,14,16,17,18	2,8,9,11,13,15,17,18	2^{-12}

Table 0.847 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	3,5,10,17	2,8,9,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	3,5,10,16,18	2,8,9,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	3,5,10,17,18	2,8,9,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	3,5,10,16	2,8,9,15	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	3,5,10,14,18	2,8,9,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	3,5,10,14,16,17	2,8,9,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	3,5,10,14	2,8,9,15	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	3,5,10,14,16,17,18	2,8,9,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	3,5,10,17,18	2,8,9,13,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	3,5,10,16	2,8,9,13	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	3,5,10,17	2,8,9,13,15,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	3,5,10,16,18	2,8,9,13,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	3,5,10,14	2,8,9,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	3,5,10,14,16,17,18	2,8,9,13,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	3,5,10,14,18	2,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	3,5,10,14,16,17	2,8,9,13,15,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	3,5,10,12,18	2,8,9,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,10,12,16,17	2,8,9,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	3,5,10,12	2,8,9,15	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,10,12,16,17,18	2,8,9,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	3,5,10,12,14,17	2,8,9,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	3,5,10,12,14,16,18	2,8,9,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	3,5,10,12,14,17,18	2,8,9,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	3,5,10,12,14,16	2,8,9,15	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	3,5,10,12	2,8,9,13	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	3,5,10,12,16,17,18	2,8,9,13,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	3,5,10,12,18	2,8,9,13,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	3,5,10,12,16,17	2,8,9,13,15,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,10,12,14,17,18	2,8,9,13,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	3,5,10,12,14,16	2,8,9,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,10,12,14,17	2,8,9,13,15,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	3,5,10,12,14,16,18	2,8,9,13,15,18	$2^{-17.5}$

Table 0.848 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	3,5,10,17,18	2,8,9,11,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	3,5,10,16	2,8,9,11	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	3,5,10,17	2,8,9,11,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	3,5,10,16,18	2,8,9,11,15,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	3,5,10,14	2,8,9,11	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	3,5,10,14,16,17,18	2,8,9,11,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,5,10,14,18	2,8,9,11,15,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	3,5,10,14,16,17	2,8,9,11,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	3,5,10,17	2,8,9,11,13,17	2^{-34}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	3,5,10,16,18	2,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	3,5,10,17,18	2,8,9,11,13,15,17,18	2^{-34}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	3,5,10,16	2,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	3,5,10,14,18	2,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	3,5,10,14,16,17	2,8,9,11,13,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,5,10,14	2,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	3,5,10,14,16,17,18	2,8,9,11,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	3,5,10,12	2,8,9,11	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	3,5,10,12,16,17,18	2,8,9,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	3,5,10,12,18	2,8,9,11,15,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	3,5,10,12,16,17	2,8,9,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	3,5,10,12,14,17,18	2,8,9,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,5,10,12,14,16	2,8,9,11	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	3,5,10,12,14,17	2,8,9,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	3,5,10,12,14,16,18	2,8,9,11,15,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	3,5,10,12,18	2,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	3,5,10,12,16,17	2,8,9,11,13,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	3,5,10,12	2,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	3,5,10,12,16,17,18	2,8,9,11,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	3,5,10,12,14,17	2,8,9,11,13,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	3,5,10,12,14,16,18	2,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	3,5,10,12,14,17,18	2,8,9,11,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	3,5,10,12,14,16	2,8,9,11,13,15	$2^{-17.5}$

Table 0.849 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	3,5,7,17	2,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	3,5,7,16,18	2,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	3,5,7,17,18	2,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	3,5,7,16	2,15	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	3,5,7,14,18	2,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	3,5,7,14,16,17	2,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	3,5,7,14	2,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	3,5,7,14,16,17,18	2,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	3,5,7,17,18	2,13,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	3,5,7,16	2,13	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	3,5,7,17	2,13,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	3,5,7,16,18	2,13,15,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	3,5,7,14	2,13	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	3,5,7,14,16,17,18	2,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	3,5,7,14,18	2,13,15,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	3,5,7,14,16,17	2,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	3,5,7,12,18	2,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	3,5,7,12,16,17	2,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	3,5,7,12	2,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	3,5,7,12,16,17,18	2,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	3,5,7,12,14,17	2,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	3,5,7,12,14,16,18	2,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	3,5,7,12,14,17,18	2,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	3,5,7,12,14,16	2,15	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	3,5,7,12	2,13	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	3,5,7,12,16,17,18	2,13,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	3,5,7,12,18	2,13,15,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	3,5,7,12,16,17	2,13,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	3,5,7,12,14,17,18	2,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	3,5,7,12,14,16	2,13	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	3,5,7,12,14,17	2,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	3,5,7,12,14,16,18	2,13,15,18	2^{-23}

Table 0.850 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	3,5,7,17,18	2,11,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	3,5,7,16	2,11	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	3,5,7,17	2,11,15,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	3,5,7,16,18	2,11,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	3,5,7,14	2,11	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	3,5,7,14,16,17,18	2,11,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	3,5,7,14,18	2,11,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	3,5,7,14,16,17	2,11,15,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	3,5,7,17	2,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	3,5,7,16,18	2,11,13,18	2^{-34}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	3,5,7,17,18	2,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	3,5,7,16	2,11,13,15	2^{-34}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,5,7,14,18	2,11,13,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	3,5,7,14,16,17	2,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	3,5,7,14	2,11,13,15	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	3,5,7,14,16,17,18	2,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	3,5,7,12	2,11	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	3,5,7,12,16,17,18	2,11,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	3,5,7,12,18	2,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	3,5,7,12,16,17	2,11,15,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	3,5,7,12,14,17,18	2,11,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	3,5,7,12,14,16	2,11	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	3,5,7,12,14,17	2,11,15,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	3,5,7,12,14,16,18	2,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	3,5,7,12,18	2,11,13,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	3,5,7,12,16,17	2,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	3,5,7,12	2,11,13,15	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	3,5,7,12,16,17,18	2,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	3,5,7,12,14,17	2,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	3,5,7,12,14,16,18	2,11,13,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	3,5,7,12,14,17,18	2,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	3,5,7,12,14,16	2,11,13,15	2^{-23}

Table 0.851 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	3,5,7,10,18	2,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,5,7,10,16,17	2,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,5,7,10	2,15	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,5,7,10,16,17,18	2,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	3,5,7,10,14,17	2,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	3,5,7,10,14,16,18	2,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	3,5,7,10,14,17,18	2,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	3,5,7,10,14,16	2,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	3,5,7,10	2,13	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	3,5,7,10,16,17,18	2,13,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	3,5,7,10,18	2,13,15,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	3,5,7,10,16,17	2,13,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	3,5,7,10,14,17,18	2,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	3,5,7,10,14,16	2,13	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	3,5,7,10,14,17	2,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	3,5,7,10,14,16,18	2,13,15,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	3,5,7,10,12,17	2,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	3,5,7,10,12,16,18	2,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	3,5,7,10,12,17,18	2,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	3,5,7,10,12,16	2,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	3,5,7,10,12,14,18	2,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	3,5,7,10,12,14,16,17	2,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	3,5,7,10,12,14	2,15	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	3,5,7,10,12,14,16,17,18	2,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,7,10,12,17,18	2,13,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	3,5,7,10,12,16	2,13	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,7,10,12,17	2,13,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	3,5,7,10,12,16,18	2,13,15,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	3,5,7,10,12,14	2,13	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	3,5,7,10,12,14,16,17,18	2,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	3,5,7,10,12,14,18	2,13,15,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	3,5,7,10,12,14,16,17	2,13,15,17	$2^{-17.5}$

Table 0.852 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	3,5,7,10	2,11	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	3,5,7,10,16,17,18	2,11,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	3,5,7,10,18	2,11,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	3,5,7,10,16,17	2,11,15,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,5,7,10,14,17,18	2,11,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	3,5,7,10,14,16	2,11	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	3,5,7,10,14,17	2,11,15,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	3,5,7,10,14,16,18	2,11,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	3,5,7,10,18	2,11,13,18	2^{-1}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	3,5,7,10,16,17	2,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	3,5,7,10	2,11,13,15	2^{-1}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	3,5,7,10,16,17,18	2,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,7,10,14,17	2,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	3,5,7,10,14,16,18	2,11,13,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,7,10,14,17,18	2,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	3,5,7,10,14,16	2,11,13,15	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	3,5,7,10,12,17,18	2,11,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	3,5,7,10,12,16	2,11	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,5,7,10,12,17	2,11,15,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	3,5,7,10,12,16,18	2,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	3,5,7,10,12,14	2,11	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	3,5,7,10,12,14,16,17,18	2,11,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	3,5,7,10,12,14,18	2,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	3,5,7,10,12,14,16,17	2,11,15,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	3,5,7,10,12,17	2,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	3,5,7,10,12,16,18	2,11,13,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	3,5,7,10,12,17,18	2,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	3,5,7,10,12,16	2,11,13,15	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	3,5,7,10,12,14,18	2,11,13,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	3,5,7,10,12,14,16,17	2,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	3,5,7,10,12,14	2,11,13,15	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	3,5,7,10,12,14,16,17,18	2,11,13,15,17,18	$2^{-17.5}$

Table 0.853 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,17,18	2,9,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	3,5,7,16	2,9	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,17	2,9,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	3,5,7,16,18	2,9,15,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	3,5,7,14	2,9	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	3,5,7,14,16,17,18	2,9,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	3,5,7,14,18	2,9,15,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	3,5,7,14,16,17	2,9,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	3,5,7,17	2,9,13,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	3,5,7,16,18	2,9,13,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	3,5,7,17,18	2,9,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	3,5,7,16	2,9,13,15	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	3,5,7,14,18	2,9,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,7,14,16,17	2,9,13,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	3,5,7,14	2,9,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	3,5,7,14,16,17,18	2,9,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	3,5,7,12	2,9	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	3,5,7,12,16,17,18	2,9,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	3,5,7,12,18	2,9,15,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	3,5,7,12,16,17	2,9,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	3,5,7,12,14,17,18	2,9,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	3,5,7,12,14,16	2,9	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,5,7,12,14,17	2,9,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	3,5,7,12,14,16,18	2,9,15,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	3,5,7,12,18	2,9,13,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	3,5,7,12,16,17	2,9,13,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	3,5,7,12	2,9,13,15	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	3,5,7,12,16,17,18	2,9,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	3,5,7,12,14,17	2,9,13,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	3,5,7,12,14,16,18	2,9,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	3,5,7,12,14,17,18	2,9,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	3,5,7,12,14,16	2,9,13,15	$2^{-17.5}$

Table 0.854 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	3,5,7,17	2,9,11,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	3,5,7,16,18	2,9,11,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,5,7,17,18	2,9,11,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	3,5,7,16	2,9,11,15	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	3,5,7,14,18	2,9,11,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	3,5,7,14,16,17	2,9,11,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	3,5,7,14	2,9,11,15	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	3,5,7,14,16,17,18	2,9,11,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	3,5,7,17,18	2,9,11,13,17,18	2^{-1}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	3,5,7,16	2,9,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	3,5,7,17	2,9,11,13,15,17	2^{-1}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	3,5,7,16,18	2,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	3,5,7,14	2,9,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	3,5,7,14,16,17,18	2,9,11,13,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	3,5,7,14,18	2,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	3,5,7,14,16,17	2,9,11,13,15,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	3,5,7,12,18	2,9,11,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	3,5,7,12,16,17	2,9,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,7,12	2,9,11,15	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	3,5,7,12,16,17,18	2,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	3,5,7,12,14,17	2,9,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	3,5,7,12,14,16,18	2,9,11,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	3,5,7,12,14,17,18	2,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	3,5,7,12,14,16	2,9,11,15	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	3,5,7,12	2,9,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	3,5,7,12,16,17,18	2,9,11,13,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	3,5,7,12,18	2,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	3,5,7,12,16,17	2,9,11,13,15,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	3,5,7,12,14,17,18	2,9,11,13,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,7,12,14,16	2,9,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	3,5,7,12,14,17	2,9,11,13,15,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,7,12,14,16,18	2,9,11,13,15,18	$2^{-17.5}$

Table 0.855 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	3,5,7,10	2,9	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	3,5,7,10,16,17,18	2,9,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	3,5,7,10,18	2,9,15,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	3,5,7,10,16,17	2,9,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	3,5,7,10,14,17,18	2,9,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	3,5,7,10,14,16	2,9	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,5,7,10,14,17	2,9,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	3,5,7,10,14,16,18	2,9,15,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	3,5,7,10,18	2,9,13,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	3,5,7,10,16,17	2,9,13,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	3,5,7,10	2,9,13,15	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	3,5,7,10,16,17,18	2,9,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	3,5,7,10,14,17	2,9,13,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	3,5,7,10,14,16,18	2,9,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	3,5,7,10,14,17,18	2,9,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	3,5,7,10,14,16	2,9,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	3,5,7,10,12,17,18	2,9,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,10,12,16	2,9	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	3,5,7,10,12,17	2,9,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,10,12,16,18	2,9,15,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,10,12,14	2,9	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	3,5,7,10,12,14,16,17,18	2,9,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,10,12,14,18	2,9,15,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	3,5,7,10,12,14,16,17	2,9,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	3,5,7,10,12,17	2,9,13,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	3,5,7,10,12,16,18	2,9,13,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	3,5,7,10,12,17,18	2,9,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	3,5,7,10,12,16	2,9,13,15	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	3,5,7,10,12,14,18	2,9,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,7,10,12,14,16,17	2,9,13,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	3,5,7,10,12,14	2,9,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,7,10,12,14,16,17,18	2,9,13,15,17,18	2^{-23}

Table 0.856 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	3,5,7,10,18	2,9,11,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	3,5,7,10,16,17	2,9,11,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	3,5,7,10	2,9,11,15	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	3,5,7,10,16,17,18	2,9,11,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	3,5,7,10,14,17	2,9,11,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	3,5,7,10,14,16,18	2,9,11,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	3,5,7,10,14,17,18	2,9,11,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	3,5,7,10,14,16	2,9,11,15	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	3,5,7,10	2,9,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	3,5,7,10,16,17,18	2,9,11,13,17,18	2^{-34}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	3,5,7,10,18	2,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	3,5,7,10,16,17	2,9,11,13,15,17	2^{-34}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	3,5,7,10,14,17,18	2,9,11,13,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	3,5,7,10,14,16	2,9,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	3,5,7,10,14,17	2,9,11,13,15,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	3,5,7,10,14,16,18	2,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	3,5,7,10,12,17	2,9,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	3,5,7,10,12,16,18	2,9,11,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	3,5,7,10,12,17,18	2,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	3,5,7,10,12,16	2,9,11,15	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5,7,10,12,14,18	2,9,11,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	3,5,7,10,12,14,16,17	2,9,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5,7,10,12,14	2,9,11,15	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	3,5,7,10,12,14,16,17,18	2,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,7,10,12,17,18	2,9,11,13,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	3,5,7,10,12,16	2,9,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	3,5,7,10,12,17	2,9,11,13,15,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	3,5,7,10,12,16,18	2,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	3,5,7,10,12,14	2,9,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	3,5,7,10,12,14,16,17,18	2,9,11,13,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	3,5,7,10,12,14,18	2,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	3,5,7,10,12,14,16,17	2,9,11,13,15,17	2^{-23}

Table 0.857 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	3,5,7,18	2,8,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	3,5,7,16,17	2,8,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	3,5,7	2,8,15	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	3,5,7,16,17,18	2,8,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	3,5,7,14,17	2,8,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	3,5,7,14,16,18	2,8,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	3,5,7,14,17,18	2,8,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,5,7,14,16	2,8,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	3,5,7	2,8,13	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	3,5,7,16,17,18	2,8,13,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	3,5,7,18	2,8,13,15,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	3,5,7,16,17	2,8,13,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	3,5,7,14,17,18	2,8,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	3,5,7,14,16	2,8,13	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	3,5,7,14,17	2,8,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	3,5,7,14,16,18	2,8,13,15,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,12,17	2,8,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	3,5,7,12,16,18	2,8,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,12,17,18	2,8,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	3,5,7,12,16	2,8,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	3,5,7,12,14,18	2,8,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,12,14,16,17	2,8,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	3,5,7,12,14	2,8,15	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,12,14,16,17,18	2,8,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	3,5,7,12,17,18	2,8,13,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	3,5,7,12,16	2,8,13	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	3,5,7,12,17	2,8,13,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	3,5,7,12,16,18	2,8,13,15,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,7,12,14	2,8,13	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5,7,12,14,16,17,18	2,8,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,7,12,14,18	2,8,13,15,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	3,5,7,12,14,16,17	2,8,13,15,17	$2^{-17.5}$

Table 0.858 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	3,5,7	2,8,11	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	3,5,7,16,17,18	2,8,11,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	3,5,7,18	2,8,11,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	3,5,7,16,17	2,8,11,15,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	3,5,7,14,17,18	2,8,11,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	3,5,7,14,16	2,8,11	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	3,5,7,14,17	2,8,11,15,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	3,5,7,14,16,18	2,8,11,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	3,5,7,18	2,8,11,13,18	2^{-34}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	3,5,7,16,17	2,8,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	3,5,7	2,8,11,13,15	2^{-34}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	3,5,7,16,17,18	2,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	3,5,7,14,17	2,8,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	3,5,7,14,16,18	2,8,11,13,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	3,5,7,14,17,18	2,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	3,5,7,14,16	2,8,11,13,15	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	3,5,7,12,17,18	2,8,11,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	3,5,7,12,16	2,8,11	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	3,5,7,12,17	2,8,11,15,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	3,5,7,12,16,18	2,8,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	3,5,7,12,14	2,8,11	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5,7,12,14,16,17,18	2,8,11,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	3,5,7,12,14,18	2,8,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5,7,12,14,16,17	2,8,11,15,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	3,5,7,12,17	2,8,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,7,12,16,18	2,8,11,13,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	3,5,7,12,17,18	2,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	3,5,7,12,16	2,8,11,13,15	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	3,5,7,12,14,18	2,8,11,13,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	3,5,7,12,14,16,17	2,8,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	3,5,7,12,14	2,8,11,13,15	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	3,5,7,12,14,16,17,18	2,8,11,13,15,17,18	$2^{-17.5}$

Table 0.859 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	3,5,7,10,17	2,8,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,10,16,18	2,8,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	3,5,7,10,17,18	2,8,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,10,16	2,8,15	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,5,7,10,14,18	2,8,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	3,5,7,10,14,16,17	2,8,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	3,5,7,10,14	2,8,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	3,5,7,10,14,16,17,18	2,8,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	3,5,7,10,17,18	2,8,13,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	3,5,7,10,16	2,8,13	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	3,5,7,10,17	2,8,13,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	3,5,7,10,16,18	2,8,13,15,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,5,7,10,14	2,8,13	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	3,5,7,10,14,16,17,18	2,8,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	3,5,7,10,14,18	2,8,13,15,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	3,5,7,10,14,16,17	2,8,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	3,5,7,10,12,18	2,8,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	3,5,7,10,12,16,17	2,8,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	3,5,7,10,12	2,8,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	3,5,7,10,12,16,17,18	2,8,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	3,5,7,10,12,14,17	2,8,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	3,5,7,10,12,14,16,18	2,8,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	3,5,7,10,12,14,17,18	2,8,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,5,7,10,12,14,16	2,8,15	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	3,5,7,10,12	2,8,13	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	3,5,7,10,12,16,17,18	2,8,13,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	3,5,7,10,12,18	2,8,13,15,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	3,5,7,10,12,16,17	2,8,13,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	3,5,7,10,12,14,17,18	2,8,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	3,5,7,10,12,14,16	2,8,13	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	3,5,7,10,12,14,17	2,8,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	3,5,7,10,12,14,16,18	2,8,13,15,18	2^{-12}

Table 0.860 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	3,5,7,10,17,18	2,8,11,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	3,5,7,10,16	2,8,11	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	3,5,7,10,17	2,8,11,15,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	3,5,7,10,16,18	2,8,11,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	3,5,7,10,14	2,8,11	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	3,5,7,10,14,16,17,18	2,8,11,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	3,5,7,10,14,18	2,8,11,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	3,5,7,10,14,16,17	2,8,11,15,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	3,5,7,10,17	2,8,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	3,5,7,10,16,18	2,8,11,13,18	2^{-1}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	3,5,7,10,17,18	2,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,5,7,10,16	2,8,11,13,15	2^{-1}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	3,5,7,10,14,18	2,8,11,13,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	3,5,7,10,14,16,17	2,8,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	3,5,7,10,14	2,8,11,13,15	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	3,5,7,10,14,16,17,18	2,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	3,5,7,10,12	2,8,11	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	3,5,7,10,12,16,17,18	2,8,11,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	3,5,7,10,12,18	2,8,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,7,10,12,16,17	2,8,11,15,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	3,5,7,10,12,14,17,18	2,8,11,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	3,5,7,10,12,14,16	2,8,11	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	3,5,7,10,12,14,17	2,8,11,15,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	3,5,7,10,12,14,16,18	2,8,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	3,5,7,10,12,18	2,8,11,13,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	3,5,7,10,12,16,17	2,8,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	3,5,7,10,12	2,8,11,13,15	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	3,5,7,10,12,16,17,18	2,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,7,10,12,14,17	2,8,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	3,5,7,10,12,14,16,18	2,8,11,13,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,7,10,12,14,17,18	2,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,5,7,10,12,14,16	2,8,11,13,15	2^{-12}

Table 0.861 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	3,5,7	2,8,9	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	3,5,7,16,17,18	2,8,9,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,5,7,18	2,8,9,15,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,5,7,16,17	2,8,9,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	3,5,7,14,17,18	2,8,9,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	3,5,7,14,16	2,8,9	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	3,5,7,14,17	2,8,9,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	3,5,7,14,16,18	2,8,9,15,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	3,5,7,18	2,8,9,13,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	3,5,7,16,17	2,8,9,13,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	3,5,7	2,8,9,13,15	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	3,5,7,16,17,18	2,8,9,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	3,5,7,14,17	2,8,9,13,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	3,5,7,14,16,18	2,8,9,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	3,5,7,14,17,18	2,8,9,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	3,5,7,14,16	2,8,9,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	3,5,7,12,17,18	2,8,9,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	3,5,7,12,16	2,8,9	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	3,5,7,12,17	2,8,9,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	3,5,7,12,16,18	2,8,9,15,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	3,5,7,12,14	2,8,9	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	3,5,7,12,14,16,17,18	2,8,9,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	3,5,7,12,14,18	2,8,9,15,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	3,5,7,12,14,16,17	2,8,9,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	3,5,7,12,17	2,8,9,13,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,7,12,16,18	2,8,9,13,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	3,5,7,12,17,18	2,8,9,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,7,12,16	2,8,9,13,15	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	3,5,7,12,14,18	2,8,9,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	3,5,7,12,14,16,17	2,8,9,13,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	3,5,7,12,14	2,8,9,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	3,5,7,12,14,16,17,18	2,8,9,13,15,17,18	2^{-12}

Table 0.862 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	3,5,7,18	2,8,9,11,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	3,5,7,16,17	2,8,9,11,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	3,5,7	2,8,9,11,15	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	3,5,7,16,17,18	2,8,9,11,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	3,5,7,14,17	2,8,9,11,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,5,7,14,16,18	2,8,9,11,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	3,5,7,14,17,18	2,8,9,11,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	3,5,7,14,16	2,8,9,11,15	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	3,5,7	2,8,9,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	3,5,7,16,17,18	2,8,9,11,13,17,18	2^{-1}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	3,5,7,18	2,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	3,5,7,16,17	2,8,9,11,13,15,17	2^{-1}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	3,5,7,14,17,18	2,8,9,11,13,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,7,14,16	2,8,9,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	3,5,7,14,17	2,8,9,11,13,15,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,7,14,16,18	2,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	3,5,7,12,17	2,8,9,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	3,5,7,12,16,18	2,8,9,11,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	3,5,7,12,17,18	2,8,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,5,7,12,16	2,8,9,11,15	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	3,5,7,12,14,18	2,8,9,11,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	3,5,7,12,14,16,17	2,8,9,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	3,5,7,12,14	2,8,9,11,15	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	3,5,7,12,14,16,17,18	2,8,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,5,7,12,17,18	2,8,9,11,13,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	3,5,7,12,16	2,8,9,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	3,5,7,12,17	2,8,9,11,13,15,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	3,5,7,12,16,18	2,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	3,5,7,12,14	2,8,9,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	3,5,7,12,14,16,17,18	2,8,9,11,13,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	3,5,7,12,14,18	2,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	3,5,7,12,14,16,17	2,8,9,11,13,15,17	2^{-12}

Table 0.863 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	3,5,7,10,17,18	2,8,9,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	3,5,7,10,16	2,8,9	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	3,5,7,10,17	2,8,9,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	3,5,7,10,16,18	2,8,9,15,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	3,5,7,10,14	2,8,9	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	3,5,7,10,14,16,17,18	2,8,9,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	3,5,7,10,14,18	2,8,9,15,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	3,5,7,10,14,16,17	2,8,9,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	3,5,7,10,17	2,8,9,13,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	3,5,7,10,16,18	2,8,9,13,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	3,5,7,10,17,18	2,8,9,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	3,5,7,10,16	2,8,9,13,15	$2^{-6.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	3,5,7,10,14,18	2,8,9,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	3,5,7,10,14,16,17	2,8,9,13,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	3,5,7,10,14	2,8,9,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	3,5,7,10,14,16,17,18	2,8,9,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	3,5,7,10,12	2,8,9	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	3,5,7,10,12,16,17,18	2,8,9,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	3,5,7,10,12,18	2,8,9,15,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	3,5,7,10,12,16,17	2,8,9,13,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	3,5,7,10,12,14,17,18	2,8,9,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	3,5,7,10,12,14,16	2,8,9	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	3,5,7,10,12,14,17	2,8,9,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	3,5,7,10,12,14,16,18	2,8,9,15,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	3,5,7,10,12,18	2,8,9,13,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	3,5,7,10,12,16,17	2,8,9,13,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	3,5,7,10,12	2,8,9,13,15	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	3,5,7,10,12,16,17,18	2,8,9,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	3,5,7,10,12,14,17	2,8,9,13,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	3,5,7,10,12,14,16,18	2,8,9,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	3,5,7,10,12,14,17,18	2,8,9,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	3,5,7,10,12,14,16	2,8,9,13,15	$2^{-17.5}$

Table 0.864 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	3,5,7,10,17	2,8,9,11,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	3,5,7,10,16,18	2,8,9,11,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	3,5,7,10,17,18	2,8,9,11,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	3,5,7,10,16	2,8,9,11,15	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	3,5,7,10,14,18	2,8,9,11,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	3,5,7,10,14,16,17	2,8,9,11,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	3,5,7,10,14	2,8,9,11,15	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	3,5,7,10,14,16,17,18	2,8,9,11,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	3,5,7,10,17,18	2,8,9,11,13,17,18	2^{-34}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	3,5,7,10,16	2,8,9,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	3,5,7,10,17	2,8,9,11,13,15,17	2^{-34}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	3,5,7,10,16,18	2,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	3,5,7,10,14	2,8,9,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,5,7,10,14,16,17,18	2,8,9,11,13,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	3,5,7,10,14,18	2,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	3,5,7,10,14,16,17	2,8,9,11,13,15,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	3,5,7,10,12,18	2,8,9,11,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	3,5,7,10,12,16,17	2,8,9,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	3,5,7,10,12	2,8,9,11,15	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	3,5,7,10,12,16,17,18	2,8,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	3,5,7,10,12,14,17	2,8,9,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	3,5,7,10,12,14,16,18	2,8,9,11,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	3,5,7,10,12,14,17,18	2,8,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	3,5,7,10,12,14,16	2,8,9,11,15	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	3,5,7,10,12	2,8,9,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	3,5,7,10,12,16,17,18	2,8,9,11,13,17,18	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	3,5,7,10,12,18	2,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	3,5,7,10,12,16,17	2,8,9,11,13,15,17	2^{-12}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	3,5,7,10,12,14,17,18	2,8,9,11,13,17,18	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	3,5,7,10,12,14,16	2,8,9,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	3,5,7,10,12,14,17	2,8,9,11,13,15,17	2^{-23}
$(0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	3,5,7,10,12,14,16,18	2,8,9,11,13,15,18	$2^{-17.5}$

Table 0.865 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5	2,6	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	3,5,16,17,18	2,6,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5,18	2,6,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,16,17	2,6,15,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	3,5,14,17,18	2,6,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	3,5,14,16	2,6	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	3,5,14,17	2,6,15,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	3,5,14,16,18	2,6,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	3,5,18	2,6,13,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	3,5,16,17	2,6,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	3,5	2,6,13,15	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	3,5,16,17,18	2,6,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,14,17	2,6,13,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	3,5,14,16,18	2,6,13,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,14,17,18	2,6,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	3,5,14,16	2,6,13,15	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,12,17,18	2,6,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	3,5,12,16	2,6	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	3,5,12,17	2,6,15,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	3,5,12,16,18	2,6,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	3,5,12,14	2,6	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	3,5,12,14,16,17,18	2,6,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	3,5,12,14,18	2,6,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	3,5,12,14,16,17	2,6,15,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	3,5,12,17	2,6,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	3,5,12,16,18	2,6,13,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	3,5,12,17,18	2,6,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	3,5,12,16	2,6,13,15	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	3,5,12,14,18	2,6,13,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	3,5,12,14,16,17	2,6,13,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	3,5,12,14	2,6,13,15	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	3,5,12,14,16,17,18	2,6,13,15,17,18	$2^{-28.5}$

Table 0.866 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	3,5,18	2,6,11,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	3,5,16,17	2,6,11,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	3,5	2,6,11,15	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	3,5,16,17,18	2,6,11,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	3,5,14,17	2,6,11,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	3,5,14,16,18	2,6,11,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	3,5,14,17,18	2,6,11,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	3,5,14,16	2,6,11,15	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	3,5	2,6,11,13	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,16,17,18	2,6,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5,18	2,6,11,13,15,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,16,17	2,6,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	3,5,14,17,18	2,6,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	3,5,14,16	2,6,11,13	2^{-34}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	3,5,14,17	2,6,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	3,5,14,16,18	2,6,11,13,15,18	2^{-34}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,5,12,17	2,6,11,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	3,5,12,16,18	2,6,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	3,5,12,17,18	2,6,11,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	3,5,12,16	2,6,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	3,5,12,14,18	2,6,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	3,5,12,14,16,17	2,6,11,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	3,5,12,14	2,6,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	3,5,12,14,16,17,18	2,6,11,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	3,5,12,17,18	2,6,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	3,5,12,16	2,6,11,13	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	3,5,12,17	2,6,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	3,5,12,16,18	2,6,11,13,15,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	3,5,12,14	2,6,11,13	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	3,5,12,14,16,17,18	2,6,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	3,5,12,14,18	2,6,11,13,15,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	3,5,12,14,16,17	2,6,11,13,15,17	$2^{-17.5}$

Table 0.867 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	3,5,10,17,18	2,6,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	3,5,10,16	2,6	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	3,5,10,17	2,6,15,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	3,5,10,16,18	2,6,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,10,14	2,6	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	3,5,10,14,16,17,18	2,6,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,10,14,18	2,6,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	3,5,10,14,16,17	2,6,15,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,5,10,17	2,6,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,10,16,18	2,6,13,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	3,5,10,17,18	2,6,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,10,16	2,6,13,15	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	3,5,10,14,18	2,6,13,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	3,5,10,14,16,17	2,6,13,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	3,5,10,14	2,6,13,15	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	3,5,10,14,16,17,18	2,6,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	3,5,10,12	2,6	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	3,5,10,12,16,17,18	2,6,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	3,5,10,12,18	2,6,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	3,5,10,12,16,17	2,6,15,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	3,5,10,12,14,17,18	2,6,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	3,5,10,12,14,16	2,6	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	3,5,10,12,14,17	2,6,15,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	3,5,10,12,14,16,18	2,6,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	3,5,10,12,18	2,6,13,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	3,5,10,12,16,17	2,6,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	3,5,10,12	2,6,13,15	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	3,5,10,12,16,17,18	2,6,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	3,5,10,12,14,17	2,6,13,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	3,5,10,12,14,16,18	2,6,13,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	3,5,10,12,14,17,18	2,6,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	3,5,10,12,14,16	2,6,13,15	2^{-12}

Table 0.868 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,5,10,17	2,6,11,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	3,5,10,16,18	2,6,11,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	3,5,10,17,18	2,6,11,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	3,5,10,16	2,6,11,15	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	3,5,10,14,18	2,6,11,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	3,5,10,14,16,17	2,6,11,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	3,5,10,14	2,6,11,15	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	3,5,10,14,16,17,18	2,6,11,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	3,5,10,17,18	2,6,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	3,5,10,16	2,6,11,13	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	3,5,10,17	2,6,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	3,5,10,16,18	2,6,11,13,15,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	3,5,10,14	2,6,11,13	2^{-1}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	3,5,10,14,16,17,18	2,6,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	3,5,10,14,18	2,6,11,13,15,18	2^{-1}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	3,5,10,14,16,17	2,6,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	3,5,10,12,18	2,6,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	3,5,10,12,16,17	2,6,11,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	3,5,10,12	2,6,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,5,10,12,16,17,18	2,6,11,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	3,5,10,12,14,17	2,6,11,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	3,5,10,12,14,16,18	2,6,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	3,5,10,12,14,17,18	2,6,11,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	3,5,10,12,14,16	2,6,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	3,5,10,12	2,6,11,13	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	3,5,10,12,16,17,18	2,6,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	3,5,10,12,18	2,6,11,13,15,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,5,10,12,16,17	2,6,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	3,5,10,12,14,17,18	2,6,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	3,5,10,12,14,16	2,6,11,13	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	3,5,10,12,14,17	2,6,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	3,5,10,12,14,16,18	2,6,11,13,15,18	2^{-23}

Table 0.869 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	3,5,18	2,6,9,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	3,5,16,17	2,6,9,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	3,5	2,6,9,15	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	3,5,16,17,18	2,6,9,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,5,14,17	2,6,9,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	3,5,14,16,18	2,6,9,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	3,5,14,17,18	2,6,9,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	3,5,14,16	2,6,9,15	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	3,5	2,6,9,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	3,5,16,17,18	2,6,9,13,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	3,5,18	2,6,9,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	3,5,16,17	2,6,9,13,15,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	3,5,14,17,18	2,6,9,13,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	3,5,14,16	2,6,9,13	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	3,5,14,17	2,6,9,13,15,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	3,5,14,16,18	2,6,9,13,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	3,5,12,17	2,6,9,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	3,5,12,16,18	2,6,9,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,5,12,17,18	2,6,9,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	3,5,12,16	2,6,9,15	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	3,5,12,14,18	2,6,9,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	3,5,12,14,16,17	2,6,9,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	3,5,12,14	2,6,9,15	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	3,5,12,14,16,17,18	2,6,9,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,12,17,18	2,6,9,13,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	3,5,12,16	2,6,9,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,12,17	2,6,9,13,15,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	3,5,12,16,18	2,6,9,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	3,5,12,14	2,6,9,13	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	3,5,12,14,16,17,18	2,6,9,13,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	3,5,12,14,18	2,6,9,13,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	3,5,12,14,16,17	2,6,9,13,15,17	2^{-12}

Table 0.870 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5	2,6,9,11	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	3,5,16,17,18	2,6,9,11,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	3,5,18	2,6,9,11,15,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	3,5,16,17	2,6,9,11,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	3,5,14,17,18	2,6,9,11,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,5,14,16	2,6,9,11	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	3,5,14,17	2,6,9,11,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	3,5,14,16,18	2,6,9,11,15,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	3,5,18	2,6,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	3,5,16,17	2,6,9,11,13,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	3,5	2,6,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	3,5,16,17,18	2,6,9,11,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,14,17	2,6,9,11,13,17	2^{-1}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	3,5,14,16,18	2,6,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,14,17,18	2,6,9,11,13,15,17,18	2^{-1}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	3,5,14,16	2,6,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	3,5,12,17,18	2,6,9,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	3,5,12,16	2,6,9,11	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	3,5,12,17	2,6,9,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	3,5,12,16,18	2,6,9,11,15,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,5,12,14	2,6,9,11	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,5,12,14,16,17,18	2,6,9,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	3,5,12,14,18	2,6,9,11,15,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	3,5,12,14,16,17	2,6,9,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	3,5,12,17	2,6,9,11,13,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	3,5,12,16,18	2,6,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	3,5,12,17,18	2,6,9,11,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	3,5,12,16	2,6,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	3,5,12,14,18	2,6,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	3,5,12,14,16,17	2,6,9,11,13,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	3,5,12,14	2,6,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	3,5,12,14,16,17,18	2,6,9,11,13,15,17,18	2^{-23}

Table 0.871 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	3,5,10,17	2,6,9,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	3,5,10,16,18	2,6,9,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	3,5,10,17,18	2,6,9,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	3,5,10,16	2,6,9,15	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	3,5,10,14,18	2,6,9,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	3,5,10,14,16,17	2,6,9,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	3,5,10,14	2,6,9,15	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	3,5,10,14,16,17,18	2,6,9,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	3,5,10,17,18	2,6,9,13,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	3,5,10,16	2,6,9,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	3,5,10,17	2,6,9,13,15,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	3,5,10,16,18	2,6,9,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	3,5,10,14	2,6,9,13	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	3,5,10,14,16,17,18	2,6,9,13,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	3,5,10,14,18	2,6,9,13,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	3,5,10,14,16,17	2,6,9,13,15,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	3,5,10,12,18	2,6,9,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	3,5,10,12,16,17	2,6,9,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	3,5,10,12	2,6,9,15	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	3,5,10,12,16,17,18	2,6,9,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	3,5,10,12,14,17	2,6,9,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	3,5,10,12,14,16,18	2,6,9,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	3,5,10,12,14,17,18	2,6,9,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	3,5,10,12,14,16	2,6,9,15	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	3,5,10,12	2,6,9,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	3,5,10,12,16,17,18	2,6,9,13,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,5,10,12,18	2,6,9,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	3,5,10,12,16,17	2,6,9,13,15,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	3,5,10,12,14,17,18	2,6,9,13,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	3,5,10,12,14,16	2,6,9,13	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	3,5,10,12,14,17	2,6,9,13,15,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	3,5,10,12,14,16,18	2,6,9,13,15,18	$2^{-28.5}$

Table 0.872 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	3,5,10,17,18	2,6,9,11,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	3,5,10,16	2,6,9,11	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	3,5,10,17	2,6,9,11,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	3,5,10,16,18	2,6,9,11,15,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	3,5,10,14	2,6,9,11	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	3,5,10,14,16,17,18	2,6,9,11,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	3,5,10,14,18	2,6,9,11,15,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	3,5,10,14,16,17	2,6,9,11,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,5,10,17	2,6,9,11,13,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	3,5,10,16,18	2,6,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,5,10,17,18	2,6,9,11,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	3,5,10,16	2,6,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	3,5,10,14,18	2,6,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	3,5,10,14,16,17	2,6,9,11,13,17	2^{-34}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	3,5,10,14	2,6,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	3,5,10,14,16,17,18	2,6,9,11,13,15,17,18	2^{-34}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	3,5,10,12	2,6,9,11	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	3,5,10,12,16,17,18	2,6,9,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	3,5,10,12,18	2,6,9,11,15,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	3,5,10,12,16,17	2,6,9,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	3,5,10,12,14,17,18	2,6,9,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	3,5,10,12,14,16	2,6,9,11	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	3,5,10,12,14,17	2,6,9,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	3,5,10,12,14,16,18	2,6,9,11,15,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	3,5,10,12,18	2,6,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	3,5,10,12,16,17	2,6,9,11,13,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	3,5,10,12	2,6,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	3,5,10,12,16,17,18	2,6,9,11,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	3,5,10,12,14,17	2,6,9,11,13,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	3,5,10,12,14,16,18	2,6,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	3,5,10,12,14,17,18	2,6,9,11,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	3,5,10,12,14,16	2,6,9,11,13,15	$2^{-17.5}$

Table 0.873 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	3,5,17,18	2,6,8,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	3,5,16	2,6,8	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	3,5,17	2,6,8,15,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	3,5,16,18	2,6,8,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	3,5,14	2,6,8	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	3,5,14,16,17,18	2,6,8,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	3,5,14,18	2,6,8,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	3,5,14,16,17	2,6,8,15,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	3,5,17	2,6,8,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	3,5,16,18	2,6,8,13,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	3,5,17,18	2,6,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	3,5,16	2,6,8,13,15	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	3,5,14,18	2,6,8,13,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	3,5,14,16,17	2,6,8,13,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	3,5,14	2,6,8,13,15	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	3,5,14,16,17,18	2,6,8,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	3,5,12	2,6,8	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	3,5,12,16,17,18	2,6,8,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	3,5,12,18	2,6,8,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	3,5,12,16,17	2,6,8,15,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	3,5,12,14,17,18	2,6,8,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	3,5,12,14,16	2,6,8	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	3,5,12,14,17	2,6,8,15,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	3,5,12,14,16,18	2,6,8,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	3,5,12,18	2,6,8,13,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	3,5,12,16,17	2,6,8,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	3,5,12	2,6,8,13,15	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,5,12,16,17,18	2,6,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	3,5,12,14,17	2,6,8,13,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	3,5,12,14,16,18	2,6,8,13,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	3,5,12,14,17,18	2,6,8,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	3,5,12,14,16	2,6,8,13,15	2^{-23}

Table 0.874 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	3,5,17	2,6,8,11,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	3,5,16,18	2,6,8,11,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	3,5,17,18	2,6,8,11,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	3,5,16	2,6,8,11,15	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	3,5,14,18	2,6,8,11,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	3,5,14,16,17	2,6,8,11,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	3,5,14	2,6,8,11,15	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	3,5,14,16,17,18	2,6,8,11,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	3,5,17,18	2,6,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	3,5,16	2,6,8,11,13	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	3,5,17	2,6,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	3,5,16,18	2,6,8,11,13,15,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	3,5,14	2,6,8,11,13	2^{-34}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	3,5,14,16,17,18	2,6,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	3,5,14,18	2,6,8,11,13,15,18	2^{-34}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	3,5,14,16,17	2,6,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	3,5,12,18	2,6,8,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	3,5,12,16,17	2,6,8,11,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	3,5,12	2,6,8,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	3,5,12,16,17,18	2,6,8,11,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	3,5,12,14,17	2,6,8,11,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	3,5,12,14,16,18	2,6,8,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	3,5,12,14,17,18	2,6,8,11,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	3,5,12,14,16	2,6,8,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	3,5,12	2,6,8,11,13	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	3,5,12,16,17,18	2,6,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	3,5,12,18	2,6,8,11,13,15,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	3,5,12,16,17	2,6,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	3,5,12,14,17,18	2,6,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	3,5,12,14,16	2,6,8,11,13	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	3,5,12,14,17	2,6,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	3,5,12,14,16,18	2,6,8,11,13,15,18	2^{-12}

Table 0.875 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	3,5,10	2,6,8	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	3,5,10,16,17,18	2,6,8,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	3,5,10,18	2,6,8,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	3,5,10,16,17	2,6,8,15,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	3,5,10,14,17,18	2,6,8,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,5,10,14,16	2,6,8	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	3,5,10,14,17	2,6,8,15,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	3,5,10,14,16,18	2,6,8,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	3,5,10,18	2,6,8,13,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	3,5,10,16,17	2,6,8,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	3,5,10	2,6,8,13,15	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	3,5,10,16,17,18	2,6,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	3,5,10,14,17	2,6,8,13,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	3,5,10,14,16,18	2,6,8,13,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	3,5,10,14,17,18	2,6,8,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	3,5,10,14,16	2,6,8,13,15	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	3,5,10,12,17,18	2,6,8,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	3,5,10,12,16	2,6,8	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	3,5,10,12,17	2,6,8,15,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,5,10,12,16,18	2,6,8,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	3,5,10,12,14	2,6,8	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	3,5,10,12,14,16,17,18	2,6,8,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	3,5,10,12,14,18	2,6,8,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	3,5,10,12,14,16,17	2,6,8,15,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	3,5,10,12,17	2,6,8,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,10,12,16,18	2,6,8,13,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	3,5,10,12,17,18	2,6,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,10,12,16	2,6,8,13,15	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	3,5,10,12,14,18	2,6,8,13,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	3,5,10,12,14,16,17	2,6,8,13,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	3,5,10,12,14	2,6,8,13,15	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	3,5,10,12,14,16,17,18	2,6,8,13,15,17,18	$2^{-6.5}$

Table 0.876 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	3,5,10,18	2,6,8,11,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,10,16,17	2,6,8,11,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	3,5,10	2,6,8,11,15	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	3,5,10,16,17,18	2,6,8,11,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	3,5,10,14,17	2,6,8,11,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	3,5,10,14,16,18	2,6,8,11,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	3,5,10,14,17,18	2,6,8,11,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	3,5,10,14,16	2,6,8,11,15	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	3,5,10	2,6,8,11,13	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	3,5,10,16,17,18	2,6,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	3,5,10,18	2,6,8,11,13,15,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	3,5,10,16,17	2,6,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	3,5,10,14,17,18	2,6,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,10,14,16	2,6,8,11,13	2^{-1}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	3,5,10,14,17	2,6,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,10,14,16,18	2,6,8,11,13,15,18	2^{-1}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	3,5,10,12,17	2,6,8,11,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	3,5,10,12,16,18	2,6,8,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	3,5,10,12,17,18	2,6,8,11,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	3,5,10,12,16	2,6,8,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,5,10,12,14,18	2,6,8,11,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,5,10,12,14,16,17	2,6,8,11,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	3,5,10,12,14	2,6,8,11,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	3,5,10,12,14,16,17,18	2,6,8,11,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	3,5,10,12,17,18	2,6,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	3,5,10,12,16	2,6,8,11,13	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	3,5,10,12,17	2,6,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	3,5,10,12,16,18	2,6,8,11,13,15,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	3,5,10,12,14	2,6,8,11,13	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	3,5,10,12,14,16,17,18	2,6,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	3,5,10,12,14,18	2,6,8,11,13,15,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	3,5,10,12,14,16,17	2,6,8,11,13,15,17	$2^{-17.5}$

Table 0.877 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	3,5,17	2,6,8,9,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	3,5,16,18	2,6,8,9,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	3,5,17,18	2,6,8,9,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	3,5,16	2,6,8,9,15	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	3,5,14,18	2,6,8,9,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,14,16,17	2,6,8,9,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	3,5,14	2,6,8,9,15	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,14,16,17,18	2,6,8,9,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,17,18	2,6,8,9,13,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,5,16	2,6,8,9,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,17	2,6,8,9,13,15,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	3,5,16,18	2,6,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	3,5,14	2,6,8,9,13	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	3,5,14,16,17,18	2,6,8,9,13,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	3,5,14,18	2,6,8,9,13,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	3,5,14,16,17	2,6,8,9,13,15,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	3,5,12,18	2,6,8,9,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	3,5,12,16,17	2,6,8,9,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	3,5,12	2,6,8,9,15	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	3,5,12,16,17,18	2,6,8,9,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	3,5,12,14,17	2,6,8,9,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	3,5,12,14,16,18	2,6,8,9,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	3,5,12,14,17,18	2,6,8,9,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	3,5,12,14,16	2,6,8,9,15	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	3,5,12	2,6,8,9,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	3,5,12,16,17,18	2,6,8,9,13,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	3,5,12,18	2,6,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	3,5,12,16,17	2,6,8,9,13,15,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	3,5,12,14,17,18	2,6,8,9,13,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	3,5,12,14,16	2,6,8,9,13	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	3,5,12,14,17	2,6,8,9,13,15,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	3,5,12,14,16,18	2,6,8,9,13,15,18	$2^{-6.5}$

Table 0.878 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	3,5,17,18	2,6,8,9,11,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,5,16	2,6,8,9,11	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	3,5,17	2,6,8,9,11,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	3,5,16,18	2,6,8,9,11,15,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	3,5,14	2,6,8,9,11	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	3,5,14,16,17,18	2,6,8,9,11,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	3,5,14,18	2,6,8,9,11,15,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	3,5,14,16,17	2,6,8,9,11,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	3,5,17	2,6,8,9,11,13,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	3,5,16,18	2,6,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	3,5,17,18	2,6,8,9,11,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	3,5,16	2,6,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	3,5,14,18	2,6,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	3,5,14,16,17	2,6,8,9,11,13,17	2^{-1}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	3,5,14	2,6,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	3,5,14,16,17,18	2,6,8,9,11,13,15,17,18	2^{-1}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	3,5,12	2,6,8,9,11	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	3,5,12,16,17,18	2,6,8,9,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,5,12,18	2,6,8,9,11,15,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	3,5,12,16,17	2,6,8,9,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	3,5,12,14,17,18	2,6,8,9,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	3,5,12,14,16	2,6,8,9,11	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	3,5,12,14,17	2,6,8,9,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	3,5,12,14,16,18	2,6,8,9,11,15,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	3,5,12,18	2,6,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	3,5,12,16,17	2,6,8,9,11,13,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,5,12	2,6,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	3,5,12,16,17,18	2,6,8,9,11,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	3,5,12,14,17	2,6,8,9,11,13,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	3,5,12,14,16,18	2,6,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	3,5,12,14,17,18	2,6,8,9,11,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	3,5,12,14,16	2,6,8,9,11,13,15	$2^{-17.5}$

Table 0.879 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	3,5,10,18	2,6,8,9,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5,10,16,17	2,6,8,9,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,10	2,6,8,9,15	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5,10,16,17,18	2,6,8,9,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	3,5,10,14,17	2,6,8,9,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	3,5,10,14,16,18	2,6,8,9,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	3,5,10,14,17,18	2,6,8,9,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	3,5,10,14,16	2,6,8,9,15	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	3,5,10	2,6,8,9,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	3,5,10,16,17,18	2,6,8,9,13,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	3,5,10,18	2,6,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	3,5,10,16,17	2,6,8,9,13,15,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	3,5,10,14,17,18	2,6,8,9,13,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,10,14,16	2,6,8,9,13	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	3,5,10,14,17	2,6,8,9,13,15,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,10,14,16,18	2,6,8,9,13,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	3,5,10,12,17	2,6,8,9,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	3,5,10,12,16,18	2,6,8,9,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	3,5,10,12,17,18	2,6,8,9,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	3,5,10,12,16	2,6,8,9,15	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	3,5,10,12,14,18	2,6,8,9,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	3,5,10,12,14,16,17	2,6,8,9,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	3,5,10,12,14	2,6,8,9,15	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	3,5,10,12,14,16,17,18	2,6,8,9,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	3,5,10,12,17,18	2,6,8,9,13,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	3,5,10,12,16	2,6,8,9,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	3,5,10,12,17	2,6,8,9,13,15,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	3,5,10,12,16,18	2,6,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	3,5,10,12,14	2,6,8,9,13	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	3,5,10,12,14,16,17,18	2,6,8,9,13,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	3,5,10,12,14,18	2,6,8,9,13,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	3,5,10,12,14,16,17	2,6,8,9,13,15,17	2^{-23}

Table 0.880 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	3,5,10	2,6,8,9,11	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	3,5,10,16,17,18	2,6,8,9,11,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,5,10,18	2,6,8,9,11,15,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	3,5,10,16,17	2,6,8,9,11,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	3,5,10,14,17,18	2,6,8,9,11,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	3,5,10,14,16	2,6,8,9,11	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	3,5,10,14,17	2,6,8,9,11,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	3,5,10,14,16,18	2,6,8,9,11,15,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,10,18	2,6,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5,10,16,17	2,6,8,9,11,13,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,5,10	2,6,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	3,5,10,16,17,18	2,6,8,9,11,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	3,5,10,14,17	2,6,8,9,11,13,17	2^{-34}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	3,5,10,14,16,18	2,6,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	3,5,10,14,17,18	2,6,8,9,11,13,15,17,18	2^{-34}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	3,5,10,14,16	2,6,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	3,5,10,12,17,18	2,6,8,9,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,5,10,12,16	2,6,8,9,11	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	3,5,10,12,17	2,6,8,9,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	3,5,10,12,16,18	2,6,8,9,11,15,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	3,5,10,12,14	2,6,8,9,11	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	3,5,10,12,14,16,17,18	2,6,8,9,11,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	3,5,10,12,14,18	2,6,8,9,11,15,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	3,5,10,12,14,16,17	2,6,8,9,11,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	3,5,10,12,17	2,6,8,9,11,13,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	3,5,10,12,16,18	2,6,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	3,5,10,12,17,18	2,6,8,9,11,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	3,5,10,12,16	2,6,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	3,5,10,12,14,18	2,6,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	3,5,10,12,14,16,17	2,6,8,9,11,13,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	3,5,10,12,14	2,6,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	3,5,10,12,14,16,17,18	2,6,8,9,11,13,15,17,18	2^{-12}

Table 0.881 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	3,5,7,18	2,6,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	3,5,7,16,17	2,6,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,7	2,6,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	3,5,7,16,17,18	2,6,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	3,5,7,14,17	2,6,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	3,5,7,14,16,18	2,6,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	3,5,7,14,17,18	2,6,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	3,5,7,14,16	2,6,15	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	3,5,7	2,6,13	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	3,5,7,16,17,18	2,6,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	3,5,7,18	2,6,13,15,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	3,5,7,16,17	2,6,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,7,14,17,18	2,6,13,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	3,5,7,14,16	2,6,13	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,7,14,17	2,6,13,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	3,5,7,14,16,18	2,6,13,15,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	3,5,7,12,17	2,6,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	3,5,7,12,16,18	2,6,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	3,5,7,12,17,18	2,6,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	3,5,7,12,16	2,6,15	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	3,5,7,12,14,18	2,6,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	3,5,7,12,14,16,17	2,6,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,5,7,12,14	2,6,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,5,7,12,14,16,17,18	2,6,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	3,5,7,12,17,18	2,6,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	3,5,7,12,16	2,6,13	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	3,5,7,12,17	2,6,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	3,5,7,12,16,18	2,6,13,15,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	3,5,7,12,14	2,6,13	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	3,5,7,12,14,16,17,18	2,6,13,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	3,5,7,12,14,18	2,6,13,15,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	3,5,7,12,14,16,17	2,6,13,15,17	$2^{-28.5}$

Table 0.882 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	3,5,7	2,6,11	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	3,5,7,16,17,18	2,6,11,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	3,5,7,18	2,6,11,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	3,5,7,16,17	2,6,11,15,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	3,5,7,14,17,18	2,6,11,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	3,5,7,14,16	2,6,11	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,5,7,14,17	2,6,11,15,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	3,5,7,14,16,18	2,6,11,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	3,5,7,18	2,6,11,13,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	3,5,7,16,17	2,6,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	3,5,7	2,6,11,13,15	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	3,5,7,16,17,18	2,6,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	3,5,7,14,17	2,6,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	3,5,7,14,16,18	2,6,11,13,18	2^{-34}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	3,5,7,14,17,18	2,6,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	3,5,7,14,16	2,6,11,13,15	2^{-34}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,5,7,12,17,18	2,6,11,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	3,5,7,12,16	2,6,11	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	3,5,7,12,17	2,6,11,15,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	3,5,7,12,16,18	2,6,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	3,5,7,12,14	2,6,11	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	3,5,7,12,14,16,17,18	2,6,11,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	3,5,7,12,14,18	2,6,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	3,5,7,12,14,16,17	2,6,11,15,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,7,12,17	2,6,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	3,5,7,12,16,18	2,6,11,13,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,7,12,17,18	2,6,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	3,5,7,12,16	2,6,11,13,15	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	3,5,7,12,14,18	2,6,11,13,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	3,5,7,12,14,16,17	2,6,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	3,5,7,12,14	2,6,11,13,15	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	3,5,7,12,14,16,17,18	2,6,11,13,15,17,18	$2^{-17.5}$

Table 0.883 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	3,5,7,10,17	2,6,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	3,5,7,10,16,18	2,6,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	3,5,7,10,17,18	2,6,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	3,5,7,10,16	2,6,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	3,5,7,10,14,18	2,6,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	3,5,7,10,14,16,17	2,6,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	3,5,7,10,14	2,6,15	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	3,5,7,10,14,16,17,18	2,6,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,5,7,10,17,18	2,6,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	3,5,7,10,16	2,6,13	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	3,5,7,10,17	2,6,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	3,5,7,10,16,18	2,6,13,15,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	3,5,7,10,14	2,6,13	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	3,5,7,10,14,16,17,18	2,6,13,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	3,5,7,10,14,18	2,6,13,15,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	3,5,7,10,14,16,17	2,6,13,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	3,5,7,10,12,18	2,6,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	3,5,7,10,12,16,17	2,6,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	3,5,7,10,12	2,6,15	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	3,5,7,10,12,16,17,18	2,6,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	3,5,7,10,12,14,17	2,6,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	3,5,7,10,12,14,16,18	2,6,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	3,5,7,10,12,14,17,18	2,6,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	3,5,7,10,12,14,16	2,6,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	3,5,7,10,12	2,6,13	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	3,5,7,10,12,16,17,18	2,6,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	3,5,7,10,12,18	2,6,13,15,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	3,5,7,10,12,16,17	2,6,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	3,5,7,10,12,14,17,18	2,6,13,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	3,5,7,10,12,14,16	2,6,13	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	3,5,7,10,12,14,17	2,6,13,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	3,5,7,10,12,14,16,18	2,6,13,15,18	2^{-12}

Table 0.884 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	3,5,7,10,17,18	2,6,11,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	3,5,7,10,16	2,6,11	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	3,5,7,10,17	2,6,11,15,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	3,5,7,10,16,18	2,6,11,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	3,5,7,10,14	2,6,11	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	3,5,7,10,14,16,17,18	2,6,11,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	3,5,7,10,14,18	2,6,11,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	3,5,7,10,14,16,17	2,6,11,15,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	3,5,7,10,17	2,6,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	3,5,7,10,16,18	2,6,11,13,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	3,5,7,10,17,18	2,6,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	3,5,7,10,16	2,6,11,13,15	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	3,5,7,10,14,18	2,6,11,13,18	2^{-1}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	3,5,7,10,14,16,17	2,6,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	3,5,7,10,14	2,6,11,13,15	2^{-1}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	3,5,7,10,14,16,17,18	2,6,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	3,5,7,10,12	2,6,11	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	3,5,7,10,12,16,17,18	2,6,11,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	3,5,7,10,12,18	2,6,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	3,5,7,10,12,16,17	2,6,11,15,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	3,5,7,10,12,14,17,18	2,6,11,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	3,5,7,10,12,14,16	2,6,11	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	3,5,7,10,12,14,17	2,6,11,15,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	3,5,7,10,12,14,16,18	2,6,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,5,7,10,12,18	2,6,11,13,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	3,5,7,10,12,16,17	2,6,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	3,5,7,10,12	2,6,11,13,15	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	3,5,7,10,12,16,17,18	2,6,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	3,5,7,10,12,14,17	2,6,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	3,5,7,10,12,14,16,18	2,6,11,13,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	3,5,7,10,12,14,17,18	2,6,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	3,5,7,10,12,14,16	2,6,11,13,15	2^{-23}

Table 0.885 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	3,5,7	2,6,9	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	3,5,7,16,17,18	2,6,9,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,18	2,6,9,15,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	3,5,7,16,17	2,6,9,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	3,5,7,14,17,18	2,6,9,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	3,5,7,14,16	2,6,9	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	3,5,7,14,17	2,6,9,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,14,16,18	2,6,9,15,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	3,5,7,18	2,6,9,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,7,16,17	2,6,9,13,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	3,5,7	2,6,9,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,7,16,17,18	2,6,9,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	3,5,7,14,17	2,6,9,13,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	3,5,7,14,16,18	2,6,9,13,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	3,5,7,14,17,18	2,6,9,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	3,5,7,14,16	2,6,9,13,15	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	3,5,7,12,17,18	2,6,9,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	3,5,7,12,16	2,6,9	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,5,7,12,17	2,6,9,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	3,5,7,12,16,18	2,6,9,15,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	3,5,7,12,14	2,6,9	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	3,5,7,12,14,16,17,18	2,6,9,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	3,5,7,12,14,18	2,6,9,15,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	3,5,7,12,14,16,17	2,6,9,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	3,5,7,12,17	2,6,9,13,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	3,5,7,12,16,18	2,6,9,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	3,5,7,12,17,18	2,6,9,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	3,5,7,12,16	2,6,9,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	3,5,7,12,14,18	2,6,9,13,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	3,5,7,12,14,16,17	2,6,9,13,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	3,5,7,12,14	2,6,9,13,15	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	3,5,7,12,14,16,17,18	2,6,9,13,15,17,18	2^{-12}

Table 0.886 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	3,5,7,18	2,6,9,11,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	3,5,7,16,17	2,6,9,11,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5,7	2,6,9,11,15	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	3,5,7,16,17,18	2,6,9,11,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	3,5,7,14,17	2,6,9,11,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	3,5,7,14,16,18	2,6,9,11,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	3,5,7,14,17,18	2,6,9,11,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	3,5,7,14,16	2,6,9,11,15	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	3,5,7	2,6,9,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	3,5,7,16,17,18	2,6,9,11,13,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	3,5,7,18	2,6,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	3,5,7,16,17	2,6,9,11,13,15,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,7,14,17,18	2,6,9,11,13,17,18	2^{-1}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	3,5,7,14,16	2,6,9,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,7,14,17	2,6,9,11,13,15,17	2^{-1}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	3,5,7,14,16,18	2,6,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	3,5,7,12,17	2,6,9,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	3,5,7,12,16,18	2,6,9,11,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	3,5,7,12,17,18	2,6,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	3,5,7,12,16	2,6,9,11,15	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	3,5,7,12,14,18	2,6,9,11,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	3,5,7,12,14,16,17	2,6,9,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	3,5,7,12,14	2,6,9,11,15	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	3,5,7,12,14,16,17,18	2,6,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	3,5,7,12,17,18	2,6,9,11,13,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	3,5,7,12,16	2,6,9,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	3,5,7,12,17	2,6,9,11,13,15,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	3,5,7,12,16,18	2,6,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	3,5,7,12,14	2,6,9,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	3,5,7,12,14,16,17,18	2,6,9,11,13,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	3,5,7,12,14,18	2,6,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	3,5,7,12,14,16,17	2,6,9,11,13,15,17	2^{-23}

Table 0.887 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	3,5,7,10,17,18	2,6,9,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	3,5,7,10,16	2,6,9	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,5,7,10,17	2,6,9,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	3,5,7,10,16,18	2,6,9,15,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	3,5,7,10,14	2,6,9	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	3,5,7,10,14,16,17,18	2,6,9,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	3,5,7,10,14,18	2,6,9,15,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	3,5,7,10,14,16,17	2,6,9,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	3,5,7,10,17	2,6,9,13,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	3,5,7,10,16,18	2,6,9,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	3,5,7,10,17,18	2,6,9,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	3,5,7,10,16	2,6,9,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	3,5,7,10,14,18	2,6,9,13,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	3,5,7,10,14,16,17	2,6,9,13,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	3,5,7,10,14	2,6,9,13,15	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	3,5,7,10,14,16,17,18	2,6,9,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	3,5,7,10,12	2,6,9	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,5,7,10,12,16,17,18	2,6,9,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	3,5,7,10,12,18	2,6,9,15,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	3,5,7,10,12,16,17	2,6,9,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,10,12,14,17,18	2,6,9,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	3,5,7,10,12,14,16	2,6,9	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,10,12,14,17	2,6,9,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	3,5,7,10,12,14,16,18	2,6,9,15,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	3,5,7,10,12,18	2,6,9,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,5,7,10,12,16,17	2,6,9,13,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	3,5,7,10,12	2,6,9,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	3,5,7,10,12,16,17,18	2,6,9,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	3,5,7,10,12,14,17	2,6,9,13,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	3,5,7,10,12,14,16,18	2,6,9,13,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	3,5,7,10,12,14,17,18	2,6,9,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	3,5,7,10,12,14,16	2,6,9,13,15	$2^{-28.5}$

Table 0.888 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	3,5,7,10,17	2,6,9,11,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	3,5,7,10,16,18	2,6,9,11,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	3,5,7,10,17,18	2,6,9,11,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	3,5,7,10,16	2,6,9,11,15	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,7,10,14,18	2,6,9,11,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	3,5,7,10,14,16,17	2,6,9,11,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,7,10,14	2,6,9,11,15	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	3,5,7,10,14,16,17,18	2,6,9,11,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,5,7,10,17,18	2,6,9,11,13,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,7,10,16	2,6,9,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,5,7,10,17	2,6,9,11,13,15,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,7,10,16,18	2,6,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	3,5,7,10,14	2,6,9,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	3,5,7,10,14,16,17,18	2,6,9,11,13,17,18	2^{-34}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	3,5,7,10,14,18	2,6,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	3,5,7,10,14,16,17	2,6,9,11,13,15,17	2^{-34}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	3,5,7,10,12,18	2,6,9,11,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	3,5,7,10,12,16,17	2,6,9,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	3,5,7,10,12	2,6,9,11,15	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	3,5,7,10,12,16,17,18	2,6,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	3,5,7,10,12,14,17	2,6,9,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	3,5,7,10,12,14,16,18	2,6,9,11,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	3,5,7,10,12,14,17,18	2,6,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	3,5,7,10,12,14,16	2,6,9,11,15	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	3,5,7,10,12	2,6,9,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	3,5,7,10,12,16,17,18	2,6,9,11,13,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	3,5,7,10,12,18	2,6,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	3,5,7,10,12,16,17	2,6,9,11,13,15,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	3,5,7,10,12,14,17,18	2,6,9,11,13,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	3,5,7,10,12,14,16	2,6,9,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	3,5,7,10,12,14,17	2,6,9,11,13,15,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	3,5,7,10,12,14,16,18	2,6,9,11,13,15,18	$2^{-17.5}$

Table 0.889 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	3,5,7,17	2,6,8,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	3,5,7,16,18	2,6,8,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	3,5,7,17,18	2,6,8,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,5,7,16	2,6,8,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	3,5,7,14,18	2,6,8,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	3,5,7,14,16,17	2,6,8,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	3,5,7,14	2,6,8,15	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	3,5,7,14,16,17,18	2,6,8,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	3,5,7,17,18	2,6,8,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	3,5,7,16	2,6,8,13	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	3,5,7,17	2,6,8,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	3,5,7,16,18	2,6,8,13,15,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	3,5,7,14	2,6,8,13	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,14,16,17,18	2,6,8,13,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	3,5,7,14,18	2,6,8,13,15,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	3,5,7,14,16,17	2,6,8,13,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,5,7,12,18	2,6,8,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	3,5,7,12,16,17	2,6,8,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	3,5,7,12	2,6,8,15	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	3,5,7,12,16,17,18	2,6,8,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	3,5,7,12,14,17	2,6,8,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,12,14,16,18	2,6,8,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	3,5,7,12,14,17,18	2,6,8,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,12,14,16	2,6,8,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,5,7,12	2,6,8,13	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	3,5,7,12,16,17,18	2,6,8,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	3,5,7,12,18	2,6,8,13,15,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	3,5,7,12,16,17	2,6,8,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	3,5,7,12,14,17,18	2,6,8,13,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	3,5,7,12,14,16	2,6,8,13	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	3,5,7,12,14,17	2,6,8,13,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	3,5,7,12,14,16,18	2,6,8,13,15,18	2^{-23}

Table 0.890 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	3,5,7,17,18	2,6,8,11,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	3,5,7,16	2,6,8,11	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	3,5,7,17	2,6,8,11,15,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	3,5,7,16,18	2,6,8,11,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	3,5,7,14	2,6,8,11	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,7,14,16,17,18	2,6,8,11,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	3,5,7,14,18	2,6,8,11,15,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,7,14,16,17	2,6,8,11,15,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,7,17	2,6,8,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	3,5,7,16,18	2,6,8,11,13,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,7,17,18	2,6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	3,5,7,16	2,6,8,11,13,15	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	3,5,7,14,18	2,6,8,11,13,18	2^{-34}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	3,5,7,14,16,17	2,6,8,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	3,5,7,14	2,6,8,11,13,15	2^{-34}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	3,5,7,14,16,17,18	2,6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	3,5,7,12	2,6,8,11	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	3,5,7,12,16,17,18	2,6,8,11,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	3,5,7,12,18	2,6,8,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	3,5,7,12,16,17	2,6,8,11,15,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	3,5,7,12,14,17,18	2,6,8,11,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	3,5,7,12,14,16	2,6,8,11	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	3,5,7,12,14,17	2,6,8,11,15,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	3,5,7,12,14,16,18	2,6,8,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	3,5,7,12,18	2,6,8,11,13,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	3,5,7,12,16,17	2,6,8,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	3,5,7,12	2,6,8,11,13,15	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	3,5,7,12,16,17,18	2,6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	3,5,7,12,14,17	2,6,8,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	3,5,7,12,14,16,18	2,6,8,11,13,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	3,5,7,12,14,17,18	2,6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	3,5,7,12,14,16	2,6,8,11,13,15	2^{-12}

Table 0.891 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	3,5,7,10,18	2,6,8,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,10,16,17	2,6,8,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	3,5,7,10	2,6,8,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,10,16,17,18	2,6,8,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,10,14,17	2,6,8,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	3,5,7,10,14,16,18	2,6,8,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,10,14,17,18	2,6,8,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	3,5,7,10,14,16	2,6,8,15	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,7,10	2,6,8,13	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	3,5,7,10,16,17,18	2,6,8,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,7,10,18	2,6,8,13,15,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	3,5,7,10,16,17	2,6,8,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	3,5,7,10,14,17,18	2,6,8,13,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	3,5,7,10,14,16	2,6,8,13	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	3,5,7,10,14,17	2,6,8,13,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	3,5,7,10,14,16,18	2,6,8,13,15,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	3,5,7,10,12,17	2,6,8,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	3,5,7,10,12,16,18	2,6,8,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	3,5,7,10,12,17,18	2,6,8,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,5,7,10,12,16	2,6,8,15	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	3,5,7,10,12,14,18	2,6,8,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	3,5,7,10,12,14,16,17	2,6,8,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	3,5,7,10,12,14	2,6,8,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	3,5,7,10,12,14,16,17,18	2,6,8,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	3,5,7,10,12,17,18	2,6,8,13,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	3,5,7,10,12,16	2,6,8,13	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	3,5,7,10,12,17	2,6,8,13,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	3,5,7,10,12,16,18	2,6,8,13,15,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	3,5,7,10,12,14	2,6,8,13	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	3,5,7,10,12,14,16,17,18	2,6,8,13,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	3,5,7,10,12,14,18	2,6,8,13,15,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	3,5,7,10,12,14,16,17	2,6,8,13,15,17	$2^{-6.5}$

Table 0.892 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	3,5,7,10	2,6,8,11	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5,7,10,16,17,18	2,6,8,11,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	3,5,7,10,18	2,6,8,11,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	3,5,7,10,16,17	2,6,8,11,15,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,10,14,17,18	2,6,8,11,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	3,5,7,10,14,16	2,6,8,11	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,10,14,17	2,6,8,11,15,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	3,5,7,10,14,16,18	2,6,8,11,15,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	3,5,7,10,18	2,6,8,11,13,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	3,5,7,10,16,17	2,6,8,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	3,5,7,10	2,6,8,11,13,15	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	3,5,7,10,16,17,18	2,6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	3,5,7,10,14,17	2,6,8,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	3,5,7,10,14,16,18	2,6,8,11,13,18	2^{-1}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	3,5,7,10,14,17,18	2,6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,7,10,14,16	2,6,8,11,13,15	2^{-1}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	3,5,7,10,12,17,18	2,6,8,11,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	3,5,7,10,12,16	2,6,8,11	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	3,5,7,10,12,17	2,6,8,11,15,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,7,10,12,16,18	2,6,8,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	3,5,7,10,12,14	2,6,8,11	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	3,5,7,10,12,14,16,17,18	2,6,8,11,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	3,5,7,10,12,14,18	2,6,8,11,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	3,5,7,10,12,14,16,17	2,6,8,11,15,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	3,5,7,10,12,17	2,6,8,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	3,5,7,10,12,16,18	2,6,8,11,13,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	3,5,7,10,12,17,18	2,6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	3,5,7,10,12,16	2,6,8,11,13,15	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	3,5,7,10,12,14,18	2,6,8,11,13,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	3,5,7,10,12,14,16,17	2,6,8,11,13,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	3,5,7,10,12,14	2,6,8,11,13,15	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	3,5,7,10,12,14,16,17,18	2,6,8,11,13,15,17,18	$2^{-17.5}$

Table 0.893 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	3,5,7,17,18	2,6,8,9,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	3,5,7,16	2,6,8,9	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	3,5,7,17	2,6,8,9,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	3,5,7,16,18	2,6,8,9,15,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	3,5,7,14	2,6,8,9	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	3,5,7,14,16,17,18	2,6,8,9,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	3,5,7,14,18	2,6,8,9,15,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	3,5,7,14,16,17	2,6,8,9,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	3,5,7,17	2,6,8,9,13,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	3,5,7,16,18	2,6,8,9,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	3,5,7,17,18	2,6,8,9,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	3,5,7,16	2,6,8,9,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	3,5,7,14,18	2,6,8,9,13,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	3,5,7,14,16,17	2,6,8,9,13,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	3,5,7,14	2,6,8,9,13,15	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	3,5,7,14,16,17,18	2,6,8,9,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	3,5,7,12	2,6,8,9	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	3,5,7,12,16,17,18	2,6,8,9,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	3,5,7,12,18	2,6,8,9,15,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	3,5,7,12,16,17	2,6,8,9,15,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	3,5,7,12,14,17,18	2,6,8,9,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	3,5,7,12,14,16	2,6,8,9	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	3,5,7,12,14,17	2,6,8,9,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	3,5,7,12,14,16,18	2,6,8,9,15,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	3,5,7,12,18	2,6,8,9,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	3,5,7,12,16,17	2,6,8,9,13,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	3,5,7,12	2,6,8,9,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	3,5,7,12,16,17,18	2,6,8,9,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	3,5,7,12,14,17	2,6,8,9,13,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	3,5,7,12,14,16,18	2,6,8,9,13,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	3,5,7,12,14,17,18	2,6,8,9,13,15,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	3,5,7,12,14,16	2,6,8,9,13,15	$2^{-6.5}$

Table 0.894 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	3,5,7,17	2,6,8,9,11,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	3,5,7,16,18	2,6,8,9,11,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	3,5,7,17,18	2,6,8,9,11,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	3,5,7,16	2,6,8,9,11,15	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	3,5,7,14,18	2,6,8,9,11,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	3,5,7,14,16,17	2,6,8,9,11,17	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	3,5,7,14	2,6,8,9,11,15	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	3,5,7,14,16,17,18	2,6,8,9,11,15,17,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	3,5,7,17,18	2,6,8,9,11,13,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	3,5,7,16	2,6,8,9,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	3,5,7,17	2,6,8,9,11,13,15,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	3,5,7,16,18	2,6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	3,5,7,14	2,6,8,9,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	3,5,7,14,16,17,18	2,6,8,9,11,13,17,18	2^{-1}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	3,5,7,14,18	2,6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	3,5,7,14,16,17	2,6,8,9,11,13,15,17	2^{-1}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	3,5,7,12,18	2,6,8,9,11,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	3,5,7,12,16,17	2,6,8,9,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	3,5,7,12	2,6,8,9,11,15	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	3,5,7,12,16,17,18	2,6,8,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	3,5,7,12,14,17	2,6,8,9,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	3,5,7,12,14,16,18	2,6,8,9,11,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	3,5,7,12,14,17,18	2,6,8,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	3,5,7,12,14,16	2,6,8,9,11,15	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	3,5,7,12	2,6,8,9,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,5,7,12,16,17,18	2,6,8,9,11,13,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	3,5,7,12,18	2,6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	3,5,7,12,16,17	2,6,8,9,11,13,15,17	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	3,5,7,12,14,17,18	2,6,8,9,11,13,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	3,5,7,12,14,16	2,6,8,9,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	3,5,7,12,14,17	2,6,8,9,11,13,15,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	3,5,7,12,14,16,18	2,6,8,9,11,13,15,18	$2^{-17.5}$

Table 0.895 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	3,5,7,10	2,6,8,9	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	3,5,7,10,16,17,18	2,6,8,9,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	3,5,7,10,18	2,6,8,9,15,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	3,5,7,10,16,17	2,6,8,9,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	3,5,7,10,14,17,18	2,6,8,9,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	3,5,7,10,14,16	2,6,8,9	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	3,5,7,10,14,17	2,6,8,9,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	3,5,7,10,14,16,18	2,6,8,9,15,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	3,5,7,10,18	2,6,8,9,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	3,5,7,10,16,17	2,6,8,9,13,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	3,5,7,10	2,6,8,9,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	3,5,7,10,16,17,18	2,6,8,9,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	3,5,7,10,14,17	2,6,8,9,13,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,7,10,14,16,18	2,6,8,9,13,18	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	3,5,7,10,14,17,18	2,6,8,9,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,7,10,14,16	2,6,8,9,13,15	$2^{-6.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	3,5,7,10,12,17,18	2,6,8,9,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	3,5,7,10,12,16	2,6,8,9	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	3,5,7,10,12,17	2,6,8,9,15,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	3,5,7,10,12,16,18	2,6,8,9,15,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	3,5,7,10,12,14	2,6,8,9	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	3,5,7,10,12,14,16,17,18	2,6,8,9,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,5,7,10,12,14,18	2,6,8,9,15,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,5,7,10,12,14,16,17	2,6,8,9,15,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	3,5,7,10,12,17	2,6,8,9,13,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	3,5,7,10,12,16,18	2,6,8,9,13,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	3,5,7,10,12,17,18	2,6,8,9,13,15,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	3,5,7,10,12,16	2,6,8,9,13,15	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	3,5,7,10,12,14,18	2,6,8,9,13,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	3,5,7,10,12,14,16,17	2,6,8,9,13,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	3,5,7,10,12,14	2,6,8,9,13,15	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	3,5,7,10,12,14,16,17,18	2,6,8,9,13,15,17,18	2^{-23}

Table 0.896 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	3,5,7,10,18	2,6,8,9,11,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,7,10,16,17	2,6,8,9,11,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	3,5,7,10	2,6,8,9,11,15	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	3,5,7,10,16,17,18	2,6,8,9,11,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	3,5,7,10,14,17	2,6,8,9,11,17	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	3,5,7,10,14,16,18	2,6,8,9,11,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	3,5,7,10,14,17,18	2,6,8,9,11,15,17,18	$2^{-28.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,5,7,10,14,16	2,6,8,9,11,15	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	3,5,7,10	2,6,8,9,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	3,5,7,10,16,17,18	2,6,8,9,11,13,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	3,5,7,10,18	2,6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	3,5,7,10,16,17	2,6,8,9,11,13,15,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	3,5,7,10,14,17,18	2,6,8,9,11,13,17,18	2^{-34}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	3,5,7,10,14,16	2,6,8,9,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	3,5,7,10,14,17	2,6,8,9,11,13,15,17	2^{-34}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	3,5,7,10,14,16,18	2,6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	3,5,7,10,12,17	2,6,8,9,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,5,7,10,12,16,18	2,6,8,9,11,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	3,5,7,10,12,17,18	2,6,8,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	3,5,7,10,12,16	2,6,8,9,11,15	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	3,5,7,10,12,14,18	2,6,8,9,11,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	3,5,7,10,12,14,16,17	2,6,8,9,11,17	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	3,5,7,10,12,14	2,6,8,9,11,15	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	3,5,7,10,12,14,16,17,18	2,6,8,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	3,5,7,10,12,17,18	2,6,8,9,11,13,17,18	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,7,10,12,16	2,6,8,9,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	3,5,7,10,12,17	2,6,8,9,11,13,15,17	2^{-23}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,7,10,12,16,18	2,6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	3,5,7,10,12,14	2,6,8,9,11,13	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	3,5,7,10,12,14,16,17,18	2,6,8,9,11,13,17,18	2^{-12}
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	3,5,7,10,12,14,18	2,6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	3,5,7,10,12,14,16,17	2,6,8,9,11,13,15,17	2^{-12}

Table 0.897 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	3,18	2,4,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	3,16,17	2,4,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	3	2,4,15	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,16,17,18	2,4,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	3,14,17	2,4,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	3,14,16,18	2,4,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	3,14,17,18	2,4,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	3,14,16	2,4,15	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	3	2,4,13	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,16,17,18	2,4,13,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	3,18	2,4,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,16,17	2,4,13,15,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	3,14,17,18	2,4,13,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	3,14,16	2,4,13	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	3,14,17	2,4,13,15,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,14,16,18	2,4,13,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	3,12,17	2,4,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	3,12,16,18	2,4,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	3,12,17,18	2,4,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	3,12,16	2,4,15	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	3,12,14,18	2,4,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	3,12,14,16,17	2,4,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	3,12,14	2,4,15	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	3,12,14,16,17,18	2,4,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	3,12,17,18	2,4,13,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	3,12,16	2,4,13	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	3,12,17	2,4,13,15,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	3,12,16,18	2,4,13,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	3,12,14	2,4,13	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	3,12,14,16,17,18	2,4,13,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	3,12,14,18	2,4,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	3,12,14,16,17	2,4,13,15,17	2^{-12}

Table 0.898 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	3	2,4,11	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	3,16,17,18	2,4,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	3,18	2,4,11,15,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	3,16,17	2,4,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	3,14,17,18	2,4,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	3,14,16	2,4,11	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	3,14,17	2,4,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	3,14,16,18	2,4,11,15,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	3,18	2,4,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	3,16,17	2,4,11,13,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	3	2,4,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	3,16,17,18	2,4,11,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	3,14,17	2,4,11,13,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	3,14,16,18	2,4,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	3,14,17,18	2,4,11,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	3,14,16	2,4,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	3,12,17,18	2,4,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	3,12,16	2,4,11	2^{-34}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	3,12,17	2,4,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	3,12,16,18	2,4,11,15,18	2^{-34}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	3,12,14	2,4,11	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	3,12,14,16,17,18	2,4,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	3,12,14,18	2,4,11,15,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	3,12,14,16,17	2,4,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	3,12,17	2,4,11,13,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	3,12,16,18	2,4,11,13,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	3,12,17,18	2,4,11,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	3,12,16	2,4,11,13,15	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	3,12,14,18	2,4,11,13,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	3,12,14,16,17	2,4,11,13,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	3,12,14	2,4,11,13,15	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	3,12,14,16,17,18	2,4,11,13,15,17,18	2^{-23}

Table 0.899 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(2)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	3,10,17	2,4,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	3,10,16,18	2,4,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	3,10,17,18	2,4,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	3,10,16	2,4,15	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	3,10,14,18	2,4,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	3,10,14,16,17	2,4,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	3,10,14	2,4,15	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	3,10,14,16,17,18	2,4,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	3,10,17,18	2,4,13,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	3,10,16	2,4,13	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	3,10,17	2,4,13,15,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	3,10,16,18	2,4,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	3,10,14	2,4,13	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	3,10,14,16,17,18	2,4,13,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	3,10,14,18	2,4,13,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	3,10,14,16,17	2,4,13,15,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	3,10,12,18	2,4,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	3,10,12,16,17	2,4,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	3,10,12	2,4,15	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	3,10,12,16,17,18	2,4,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	3,10,12,14,17	2,4,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	3,10,12,14,16,18	2,4,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	3,10,12,14,17,18	2,4,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	3,10,12,14,16	2,4,15	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	3,10,12	2,4,13	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	3,10,12,16,17,18	2,4,13,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	3,10,12,18	2,4,13,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,10,12,16,17	2,4,13,15,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	3,10,12,14,17,18	2,4,13,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	3,10,12,14,16	2,4,13	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	3,10,12,14,17	2,4,13,15,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	3,10,12,14,16,18	2,4,13,15,18	$2^{-17.5}$

Table 0.900 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	3,10,17,18	2,4,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	3,10,16	2,4,11	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	3,10,17	2,4,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	3,10,16,18	2,4,11,15,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	3,10,14	2,4,11	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	3,10,14,16,17,18	2,4,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	3,10,14,18	2,4,11,15,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	3,10,14,16,17	2,4,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	3,10,17	2,4,11,13,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	3,10,16,18	2,4,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	3,10,17,18	2,4,11,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	3,10,16	2,4,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	3,10,14,18	2,4,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	3,10,14,16,17	2,4,11,13,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	3,10,14	2,4,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	3,10,14,16,17,18	2,4,11,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	3,10,12	2,4,11	2^{-1}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	3,10,12,16,17,18	2,4,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,10,12,18	2,4,11,15,18	2^{-1}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	3,10,12,16,17	2,4,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	3,10,12,14,17,18	2,4,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	3,10,12,14,16	2,4,11	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	3,10,12,14,17	2,4,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	3,10,12,14,16,18	2,4,11,15,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	3,10,12,18	2,4,11,13,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	3,10,12,16,17	2,4,11,13,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	3,10,12	2,4,11,13,15	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	3,10,12,16,17,18	2,4,11,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	3,10,12,14,17	2,4,11,13,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	3,10,12,14,16,18	2,4,11,13,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	3,10,12,14,17,18	2,4,11,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	3,10,12,14,16	2,4,11,13,15	$2^{-6.5}$

Table 0.901 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	3	2,4,9	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	3,16,17,18	2,4,9,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	3,18	2,4,9,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	3,16,17	2,4,9,15,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	3,14,17,18	2,4,9,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	3,14,16	2,4,9	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	3,14,17	2,4,9,15,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	3,14,16,18	2,4,9,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	3,18	2,4,9,13,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	3,16,17	2,4,9,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	3	2,4,9,13,15	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	3,16,17,18	2,4,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	3,14,17	2,4,9,13,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	3,14,16,18	2,4,9,13,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	3,14,17,18	2,4,9,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	3,14,16	2,4,9,13,15	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	3,12,17,18	2,4,9,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	3,12,16	2,4,9	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	3,12,17	2,4,9,15,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	3,12,16,18	2,4,9,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	3,12,14	2,4,9	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	3,12,14,16,17,18	2,4,9,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	3,12,14,18	2,4,9,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	3,12,14,16,17	2,4,9,15,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	3,12,17	2,4,9,13,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	3,12,16,18	2,4,9,13,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	3,12,17,18	2,4,9,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	3,12,16	2,4,9,13,15	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	3,12,14,18	2,4,9,13,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	3,12,14,16,17	2,4,9,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	3,12,14	2,4,9,13,15	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	3,12,14,16,17,18	2,4,9,13,15,17,18	$2^{-17.5}$

Table 0.902 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	3,18	2,4,9,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	3,16,17	2,4,9,11,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	3	2,4,9,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	3,16,17,18	2,4,9,11,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	3,14,17	2,4,9,11,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	3,14,16,18	2,4,9,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	3,14,17,18	2,4,9,11,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	3,14,16	2,4,9,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	3	2,4,9,11,13	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	3,16,17,18	2,4,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,18	2,4,9,11,13,15,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	3,16,17	2,4,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	3,14,17,18	2,4,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	3,14,16	2,4,9,11,13	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	3,14,17	2,4,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	3,14,16,18	2,4,9,11,13,15,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	3,12,17	2,4,9,11,17	2^{-1}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	3,12,16,18	2,4,9,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	3,12,17,18	2,4,9,11,15,17,18	2^{-1}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	3,12,16	2,4,9,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	3,12,14,18	2,4,9,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	3,12,14,16,17	2,4,9,11,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	3,12,14	2,4,9,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	3,12,14,16,17,18	2,4,9,11,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	3,12,17,18	2,4,9,11,13,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	3,12,16	2,4,9,11,13	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	3,12,17	2,4,9,11,13,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	3,12,16,18	2,4,9,11,13,15,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	3,12,14	2,4,9,11,13	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	3,12,14,16,17,18	2,4,9,11,13,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	3,12,14,18	2,4,9,11,13,15,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	3,12,14,16,17	2,4,9,11,13,15,17	$2^{-6.5}$

Table 0.903 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	3,10,17,18	2,4,9,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	3,10,16	2,4,9	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	3,10,17	2,4,9,15,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	3,10,16,18	2,4,9,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,10,14	2,4,9	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,10,14,16,17,18	2,4,9,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	3,10,14,18	2,4,9,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	3,10,14,16,17	2,4,9,15,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	3,10,17	2,4,9,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	3,10,16,18	2,4,9,13,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	3,10,17,18	2,4,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	3,10,16	2,4,9,13,15	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	3,10,14,18	2,4,9,13,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	3,10,14,16,17	2,4,9,13,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	3,10,14	2,4,9,13,15	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	3,10,14,16,17,18	2,4,9,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	3,10,12	2,4,9	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	3,10,12,16,17,18	2,4,9,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	3,10,12,18	2,4,9,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	3,10,12,16,17	2,4,9,15,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	3,10,12,14,17,18	2,4,9,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	3,10,12,14,16	2,4,9	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	3,10,12,14,17	2,4,9,15,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	3,10,12,14,16,18	2,4,9,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	3,10,12,18	2,4,9,13,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	3,10,12,16,17	2,4,9,13,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	3,10,12	2,4,9,13,15	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	3,10,12,16,17,18	2,4,9,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	3,10,12,14,17	2,4,9,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	3,10,12,14,16,18	2,4,9,13,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,10,12,14,17,18	2,4,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	3,10,12,14,16	2,4,9,13,15	2^{-12}

Table 0.904 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	3,10,17	2,4,9,11,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	3,10,16,18	2,4,9,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,10,17,18	2,4,9,11,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	3,10,16	2,4,9,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	3,10,14,18	2,4,9,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	3,10,14,16,17	2,4,9,11,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	3,10,14	2,4,9,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	3,10,14,16,17,18	2,4,9,11,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	3,10,17,18	2,4,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	3,10,16	2,4,9,11,13	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,10,17	2,4,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	3,10,16,18	2,4,9,11,13,15,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	3,10,14	2,4,9,11,13	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	3,10,14,16,17,18	2,4,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	3,10,14,18	2,4,9,11,13,15,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	3,10,14,16,17	2,4,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	3,10,12,18	2,4,9,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	3,10,12,16,17	2,4,9,11,17	2^{-34}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	3,10,12	2,4,9,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	3,10,12,16,17,18	2,4,9,11,15,17,18	2^{-34}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,10,12,14,17	2,4,9,11,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	3,10,12,14,16,18	2,4,9,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	3,10,12,14,17,18	2,4,9,11,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	3,10,12,14,16	2,4,9,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	3,10,12	2,4,9,11,13	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	3,10,12,16,17,18	2,4,9,11,13,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	3,10,12,18	2,4,9,11,13,15,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	3,10,12,16,17	2,4,9,11,13,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	3,10,12,14,17,18	2,4,9,11,13,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	3,10,12,14,16	2,4,9,11,13	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	3,10,12,14,17	2,4,9,11,13,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	3,10,12,14,16,18	2,4,9,11,13,15,18	2^{-23}

Table 0.905 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	3,17	2,4,8,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	3,16,18	2,4,8,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	3,17,18	2,4,8,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	3,16	2,4,8,15	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,14,18	2,4,8,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,14,16,17	2,4,8,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,14	2,4,8,15	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	3,14,16,17,18	2,4,8,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	3,17,18	2,4,8,13,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	3,16	2,4,8,13	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	3,17	2,4,8,13,15,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	3,16,18	2,4,8,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	3,14	2,4,8,13	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	3,14,16,17,18	2,4,8,13,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	3,14,18	2,4,8,13,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	3,14,16,17	2,4,8,13,15,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	3,12,18	2,4,8,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	3,12,16,17	2,4,8,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	3,12	2,4,8,15	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	3,12,16,17,18	2,4,8,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	3,12,14,17	2,4,8,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	3,12,14,16,18	2,4,8,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	3,12,14,17,18	2,4,8,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	3,12,14,16	2,4,8,15	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	3,12	2,4,8,13	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	3,12,16,17,18	2,4,8,13,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	3,12,18	2,4,8,13,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	3,12,16,17	2,4,8,13,15,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	3,12,14,17,18	2,4,8,13,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	3,12,14,16	2,4,8,13	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	3,12,14,17	2,4,8,13,15,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,12,14,16,18	2,4,8,13,15,18	$2^{-17.5}$

Table 0.906 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	3,17,18	2,4,8,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	3,16	2,4,8,11	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	3,17	2,4,8,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,16,18	2,4,8,11,15,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	3,14	2,4,8,11	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	3,14,16,17,18	2,4,8,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	3,14,18	2,4,8,11,15,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	3,14,16,17	2,4,8,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	3,17	2,4,8,11,13,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	3,16,18	2,4,8,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	3,17,18	2,4,8,11,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,16	2,4,8,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	3,14,18	2,4,8,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	3,14,16,17	2,4,8,11,13,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	3,14	2,4,8,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	3,14,16,17,18	2,4,8,11,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	3,12	2,4,8,11	2^{-34}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	3,12,16,17,18	2,4,8,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	3,12,18	2,4,8,11,15,18	2^{-34}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	3,12,16,17	2,4,8,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	3,12,14,17,18	2,4,8,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,12,14,16	2,4,8,11	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	3,12,14,17	2,4,8,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	3,12,14,16,18	2,4,8,11,15,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	3,12,18	2,4,8,11,13,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	3,12,16,17	2,4,8,11,13,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	3,12	2,4,8,11,13,15	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	3,12,16,17,18	2,4,8,11,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	3,12,14,17	2,4,8,11,13,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	3,12,14,16,18	2,4,8,11,13,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,12,14,17,18	2,4,8,11,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	3,12,14,16	2,4,8,11,13,15	$2^{-28.5}$

Table 0.907 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	3,10,18	2,4,8,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	3,10,16,17	2,4,8,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	3,10	2,4,8,15	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	3,10,16,17,18	2,4,8,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	3,10,14,17	2,4,8,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	3,10,14,16,18	2,4,8,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	3,10,14,17,18	2,4,8,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	3,10,14,16	2,4,8,15	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	3,10	2,4,8,13	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	3,10,16,17,18	2,4,8,13,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	3,10,18	2,4,8,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	3,10,16,17	2,4,8,13,15,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	3,10,14,17,18	2,4,8,13,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	3,10,14,16	2,4,8,13	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	3,10,14,17	2,4,8,13,15,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	3,10,14,16,18	2,4,8,13,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	3,10,12,17	2,4,8,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	3,10,12,16,18	2,4,8,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	3,10,12,17,18	2,4,8,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	3,10,12,16	2,4,8,15	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	3,10,12,14,18	2,4,8,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	3,10,12,14,16,17	2,4,8,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	3,10,12,14	2,4,8,15	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	3,10,12,14,16,17,18	2,4,8,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	3,10,12,17,18	2,4,8,13,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	3,10,12,16	2,4,8,13	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	3,10,12,17	2,4,8,13,15,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	3,10,12,16,18	2,4,8,13,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	3,10,12,14	2,4,8,13	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	3,10,12,14,16,17,18	2,4,8,13,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	3,10,12,14,18	2,4,8,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	3,10,12,14,16,17	2,4,8,13,15,17	2^{-23}

Table 0.908 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	3,10	2,4,8,11	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	3,10,16,17,18	2,4,8,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	3,10,18	2,4,8,11,15,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	3,10,16,17	2,4,8,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	3,10,14,17,18	2,4,8,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	3,10,14,16	2,4,8,11	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	3,10,14,17	2,4,8,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	3,10,14,16,18	2,4,8,11,15,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	3,10,18	2,4,8,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	3,10,16,17	2,4,8,11,13,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	3,10	2,4,8,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,10,16,17,18	2,4,8,11,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	3,10,14,17	2,4,8,11,13,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	3,10,14,16,18	2,4,8,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	3,10,14,17,18	2,4,8,11,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	3,10,14,16	2,4,8,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	3,10,12,17,18	2,4,8,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	3,10,12,16	2,4,8,11	2^{-1}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	3,10,12,17	2,4,8,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	3,10,12,16,18	2,4,8,11,15,18	2^{-1}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	3,10,12,14	2,4,8,11	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	3,10,12,14,16,17,18	2,4,8,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	3,10,12,14,18	2,4,8,11,15,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	3,10,12,14,16,17	2,4,8,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	3,10,12,17	2,4,8,11,13,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	3,10,12,16,18	2,4,8,11,13,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	3,10,12,17,18	2,4,8,11,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	3,10,12,16	2,4,8,11,13,15	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	3,10,12,14,18	2,4,8,11,13,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	3,10,12,14,16,17	2,4,8,11,13,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	3,10,12,14	2,4,8,11,13,15	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	3,10,12,14,16,17,18	2,4,8,11,13,15,17,18	2^{-12}

Table 0.909 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	3,17,18	2,4,8,9,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,16	2,4,8,9	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	3,17	2,4,8,9,15,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	3,16,18	2,4,8,9,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	3,14	2,4,8,9	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	3,14,16,17,18	2,4,8,9,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	3,14,18	2,4,8,9,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	3,14,16,17	2,4,8,9,15,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	3,17	2,4,8,9,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	3,16,18	2,4,8,9,13,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	3,17,18	2,4,8,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	3,16	2,4,8,9,13,15	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	3,14,18	2,4,8,9,13,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	3,14,16,17	2,4,8,9,13,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	3,14	2,4,8,9,13,15	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	3,14,16,17,18	2,4,8,9,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	3,12	2,4,8,9	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	3,12,16,17,18	2,4,8,9,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	3,12,18	2,4,8,9,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	3,12,16,17	2,4,8,9,15,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	3,12,14,17,18	2,4,8,9,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	3,12,14,16	2,4,8,9	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	3,12,14,17	2,4,8,9,15,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	3,12,14,16,18	2,4,8,9,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	3,12,18	2,4,8,9,13,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	3,12,16,17	2,4,8,9,13,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,12	2,4,8,9,13,15	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	3,12,16,17,18	2,4,8,9,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	3,12,14,17	2,4,8,9,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	3,12,14,16,18	2,4,8,9,13,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	3,12,14,17,18	2,4,8,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	3,12,14,16	2,4,8,9,13,15	2^{-23}

Table 0.910 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	3,17	2,4,8,9,11,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	3,16,18	2,4,8,9,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	3,17,18	2,4,8,9,11,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	3,16	2,4,8,9,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	3,14,18	2,4,8,9,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	3,14,16,17	2,4,8,9,11,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	3,14	2,4,8,9,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	3,14,16,17,18	2,4,8,9,11,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	3,17,18	2,4,8,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	3,16	2,4,8,9,11,13	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	3,17	2,4,8,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	3,16,18	2,4,8,9,11,13,15,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	3,14	2,4,8,9,11,13	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	3,14,16,17,18	2,4,8,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	3,14,18	2,4,8,9,11,13,15,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	3,14,16,17	2,4,8,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	3,12,18	2,4,8,9,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	3,12,16,17	2,4,8,9,11,17	2^{-1}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	3,12	2,4,8,9,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,12,16,17,18	2,4,8,9,11,15,17,18	2^{-1}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	3,12,14,17	2,4,8,9,11,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	3,12,14,16,18	2,4,8,9,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	3,12,14,17,18	2,4,8,9,11,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	3,12,14,16	2,4,8,9,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	3,12	2,4,8,9,11,13	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	3,12,16,17,18	2,4,8,9,11,13,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	3,12,18	2,4,8,9,11,13,15,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	3,12,16,17	2,4,8,9,11,13,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	3,12,14,17,18	2,4,8,9,11,13,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	3,12,14,16	2,4,8,9,11,13	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	3,12,14,17	2,4,8,9,11,13,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	3,12,14,16,18	2,4,8,9,11,13,15,18	2^{-12}

Table 0.911 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	3,10	2,4,8,9	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	3,10,16,17,18	2,4,8,9,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,10,18	2,4,8,9,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	3,10,16,17	2,4,8,9,15,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	3,10,14,17,18	2,4,8,9,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	3,10,14,16	2,4,8,9	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	3,10,14,17	2,4,8,9,15,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	3,10,14,16,18	2,4,8,9,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	3,10,18	2,4,8,9,13,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	3,10,16,17	2,4,8,9,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,10	2,4,8,9,13,15	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	3,10,16,17,18	2,4,8,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	3,10,14,17	2,4,8,9,13,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	3,10,14,16,18	2,4,8,9,13,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	3,10,14,17,18	2,4,8,9,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	3,10,14,16	2,4,8,9,13,15	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	3,10,12,17,18	2,4,8,9,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,10,12,16	2,4,8,9	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	3,10,12,17	2,4,8,9,15,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	3,10,12,16,18	2,4,8,9,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	3,10,12,14	2,4,8,9	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	3,10,12,14,16,17,18	2,4,8,9,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	3,10,12,14,18	2,4,8,9,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	3,10,12,14,16,17	2,4,8,9,15,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	3,10,12,17	2,4,8,9,13,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	3,10,12,16,18	2,4,8,9,13,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	3,10,12,17,18	2,4,8,9,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	3,10,12,16	2,4,8,9,13,15	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	3,10,12,14,18	2,4,8,9,13,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	3,10,12,14,16,17	2,4,8,9,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	3,10,12,14	2,4,8,9,13,15	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	3,10,12,14,16,17,18	2,4,8,9,13,15,17,18	$2^{-17.5}$

Table 0.912 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	3,10,18	2,4,8,9,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	3,10,16,17	2,4,8,9,11,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	3,10	2,4,8,9,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	3,10,16,17,18	2,4,8,9,11,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	3,10,14,17	2,4,8,9,11,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	3,10,14,16,18	2,4,8,9,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	3,10,14,17,18	2,4,8,9,11,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	3,10,14,16	2,4,8,9,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	3,10	2,4,8,9,11,13	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	3,10,16,17,18	2,4,8,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	3,10,18	2,4,8,9,11,13,15,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	3,10,16,17	2,4,8,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	3,10,14,17,18	2,4,8,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	3,10,14,16	2,4,8,9,11,13	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	3,10,14,17	2,4,8,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	3,10,14,16,18	2,4,8,9,11,13,15,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	3,10,12,17	2,4,8,9,11,17	2^{-34}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	3,10,12,16,18	2,4,8,9,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	3,10,12,17,18	2,4,8,9,11,15,17,18	2^{-34}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	3,10,12,16	2,4,8,9,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	3,10,12,14,18	2,4,8,9,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	3,10,12,14,16,17	2,4,8,9,11,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	3,10,12,14	2,4,8,9,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	3,10,12,14,16,17,18	2,4,8,9,11,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	3,10,12,17,18	2,4,8,9,11,13,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	3,10,12,16	2,4,8,9,11,13	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	3,10,12,17	2,4,8,9,11,13,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	3,10,12,16,18	2,4,8,9,11,13,15,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	3,10,12,14	2,4,8,9,11,13	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	3,10,12,14,16,17,18	2,4,8,9,11,13,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	3,10,12,14,18	2,4,8,9,11,13,15,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	3,10,12,14,16,17	2,4,8,9,11,13,15,17	$2^{-28.5}$

Table 0.913 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	3,7	2,4	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	3,7,16,17,18	2,4,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	3,7,18	2,4,15,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	3,7,16,17	2,4,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	3,7,14,17,18	2,4,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	3,7,14,16	2,4	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	3,7,14,17	2,4,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	3,7,14,16,18	2,4,15,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,7,18	2,4,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	3,7,16,17	2,4,13,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	3,7	2,4,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	3,7,16,17,18	2,4,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	3,7,14,17	2,4,13,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	3,7,14,16,18	2,4,13,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	3,7,14,17,18	2,4,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	3,7,14,16	2,4,13,15	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	3,7,12,17,18	2,4,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	3,7,12,16	2,4	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	3,7,12,17	2,4,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	3,7,12,16,18	2,4,15,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	3,7,12,14	2,4	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	3,7,12,14,16,17,18	2,4,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	3,7,12,14,18	2,4,15,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	3,7,12,14,16,17	2,4,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	3,7,12,17	2,4,13,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	3,7,12,16,18	2,4,13,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	3,7,12,17,18	2,4,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	3,7,12,16	2,4,13,15	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	3,7,12,14,18	2,4,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	3,7,12,14,16,17	2,4,13,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	3,7,12,14	2,4,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	3,7,12,14,16,17,18	2,4,13,15,17,18	2^{-12}

Table 0.914 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	3,7,18	2,4,11,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	3,7,16,17	2,4,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	3,7	2,4,11,15	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	3,7,16,17,18	2,4,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	3,7,14,17	2,4,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	3,7,14,16,18	2,4,11,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	3,7,14,17,18	2,4,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	3,7,14,16	2,4,11,15	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	3,7	2,4,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	3,7,16,17,18	2,4,11,13,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	3,7,18	2,4,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	3,7,16,17	2,4,11,13,15,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	3,7,14,17,18	2,4,11,13,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	3,7,14,16	2,4,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	3,7,14,17	2,4,11,13,15,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	3,7,14,16,18	2,4,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	3,7,12,17	2,4,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	3,7,12,16,18	2,4,11,18	2^{-34}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	3,7,12,17,18	2,4,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	3,7,12,16	2,4,11,15	2^{-34}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	3,7,12,14,18	2,4,11,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	3,7,12,14,16,17	2,4,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	3,7,12,14	2,4,11,15	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	3,7,12,14,16,17,18	2,4,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	3,7,12,17,18	2,4,11,13,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	3,7,12,16	2,4,11,13	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	3,7,12,17	2,4,11,13,15,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	3,7,12,16,18	2,4,11,13,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	3,7,12,14	2,4,11,13	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	3,7,12,14,16,17,18	2,4,11,13,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	3,7,12,14,18	2,4,11,13,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	3,7,12,14,16,17	2,4,11,13,15,17	2^{-23}

Table 0.915 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,7,10,17,18	2,4,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	3,7,10,16	2,4	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	3,7,10,17	2,4,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	3,7,10,16,18	2,4,15,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	3,7,10,14	2,4	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	3,7,10,14,16,17,18	2,4,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	3,7,10,14,18	2,4,15,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	3,7,10,14,16,17	2,4,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,7,10,17	2,4,13,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	3,7,10,16,18	2,4,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	3,7,10,17,18	2,4,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	3,7,10,16	2,4,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	3,7,10,14,18	2,4,13,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	3,7,10,14,16,17	2,4,13,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	3,7,10,14	2,4,13,15	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	3,7,10,14,16,17,18	2,4,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	3,7,10,12	2,4	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	3,7,10,12,16,17,18	2,4,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	3,7,10,12,18	2,4,15,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	3,7,10,12,16,17	2,4,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	3,7,10,12,14,17,18	2,4,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	3,7,10,12,14,16	2,4	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,7,10,12,14,17	2,4,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	3,7,10,12,14,16,18	2,4,15,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	3,7,10,12,18	2,4,13,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	3,7,10,12,16,17	2,4,13,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	3,7,10,12	2,4,13,15	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	3,7,10,12,16,17,18	2,4,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	3,7,10,12,14,17	2,4,13,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	3,7,10,12,14,16,18	2,4,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	3,7,10,12,14,17,18	2,4,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	3,7,10,12,14,16	2,4,13,15	$2^{-17.5}$

Table 0.916 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	3,7,10,17	2,4,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	3,7,10,16,18	2,4,11,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	3,7,10,17,18	2,4,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	3,7,10,16	2,4,11,15	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	3,7,10,14,18	2,4,11,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	3,7,10,14,16,17	2,4,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,7,10,14	2,4,11,15	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,7,10,14,16,17,18	2,4,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	3,7,10,17,18	2,4,11,13,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	3,7,10,16	2,4,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	3,7,10,17	2,4,11,13,15,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	3,7,10,16,18	2,4,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	3,7,10,14	2,4,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	3,7,10,14,16,17,18	2,4,11,13,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	3,7,10,14,18	2,4,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	3,7,10,14,16,17	2,4,11,13,15,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	3,7,10,12,18	2,4,11,18	2^{-1}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	3,7,10,12,16,17	2,4,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	3,7,10,12	2,4,11,15	2^{-1}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	3,7,10,12,16,17,18	2,4,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	3,7,10,12,14,17	2,4,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	3,7,10,12,14,16,18	2,4,11,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	3,7,10,12,14,17,18	2,4,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	3,7,10,12,14,16	2,4,11,15	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	3,7,10,12	2,4,11,13	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	3,7,10,12,16,17,18	2,4,11,13,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	3,7,10,12,18	2,4,11,13,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	3,7,10,12,16,17	2,4,11,13,15,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,7,10,12,14,17,18	2,4,11,13,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	3,7,10,12,14,16	2,4,11,13	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	3,7,10,12,14,17	2,4,11,13,15,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	3,7,10,12,14,16,18	2,4,11,13,15,18	$2^{-6.5}$

Table 0.917 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	3,7,18	2,4,9,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	3,7,16,17	2,4,9,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	3,7	2,4,9,15	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	3,7,16,17,18	2,4,9,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	3,7,14,17	2,4,9,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	3,7,14,16,18	2,4,9,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	3,7,14,17,18	2,4,9,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	3,7,14,16	2,4,9,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	3,7	2,4,9,13	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	3,7,16,17,18	2,4,9,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	3,7,18	2,4,9,13,15,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,7,16,17	2,4,9,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	3,7,14,17,18	2,4,9,13,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	3,7,14,16	2,4,9,13	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	3,7,14,17	2,4,9,13,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	3,7,14,16,18	2,4,9,13,15,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	3,7,12,17	2,4,9,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	3,7,12,16,18	2,4,9,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	3,7,12,17,18	2,4,9,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	3,7,12,16	2,4,9,15	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	3,7,12,14,18	2,4,9,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	3,7,12,14,16,17	2,4,9,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	3,7,12,14	2,4,9,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	3,7,12,14,16,17,18	2,4,9,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	3,7,12,17,18	2,4,9,13,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	3,7,12,16	2,4,9,13	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	3,7,12,17	2,4,9,13,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	3,7,12,16,18	2,4,9,13,15,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	3,7,12,14	2,4,9,13	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	3,7,12,14,16,17,18	2,4,9,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	3,7,12,14,18	2,4,9,13,15,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	3,7,12,14,16,17	2,4,9,13,15,17	$2^{-17.5}$

Table 0.918 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	3,7	2,4,9,11	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,7,16,17,18	2,4,9,11,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	3,7,18	2,4,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	3,7,16,17	2,4,9,11,15,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	3,7,14,17,18	2,4,9,11,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	3,7,14,16	2,4,9,11	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	3,7,14,17	2,4,9,11,15,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	3,7,14,16,18	2,4,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	3,7,18	2,4,9,11,13,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,7,16,17	2,4,9,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	3,7	2,4,9,11,13,15	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	3,7,16,17,18	2,4,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	3,7,14,17	2,4,9,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	3,7,14,16,18	2,4,9,11,13,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	3,7,14,17,18	2,4,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	3,7,14,16	2,4,9,11,13,15	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	3,7,12,17,18	2,4,9,11,17,18	2^{-1}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	3,7,12,16	2,4,9,11	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,7,12,17	2,4,9,11,15,17	2^{-1}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	3,7,12,16,18	2,4,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	3,7,12,14	2,4,9,11	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	3,7,12,14,16,17,18	2,4,9,11,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	3,7,12,14,18	2,4,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	3,7,12,14,16,17	2,4,9,11,15,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	3,7,12,17	2,4,9,11,13,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	3,7,12,16,18	2,4,9,11,13,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	3,7,12,17,18	2,4,9,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	3,7,12,16	2,4,9,11,13,15	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	3,7,12,14,18	2,4,9,11,13,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	3,7,12,14,16,17	2,4,9,11,13,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	3,7,12,14	2,4,9,11,13,15	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	3,7,12,14,16,17,18	2,4,9,11,13,15,17,18	$2^{-6.5}$

Table 0.919 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	3,7,10,17	2,4,9,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	3,7,10,16,18	2,4,9,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	3,7,10,17,18	2,4,9,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	3,7,10,16	2,4,9,15	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	3,7,10,14,18	2,4,9,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	3,7,10,14,16,17	2,4,9,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	3,7,10,14	2,4,9,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	3,7,10,14,16,17,18	2,4,9,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	3,7,10,17,18	2,4,9,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	3,7,10,16	2,4,9,13	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	3,7,10,17	2,4,9,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	3,7,10,16,18	2,4,9,13,15,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	3,7,10,14	2,4,9,13	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	3,7,10,14,16,17,18	2,4,9,13,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	3,7,10,14,18	2,4,9,13,15,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	3,7,10,14,16,17	2,4,9,13,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,7,10,12,18	2,4,9,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	3,7,10,12,16,17	2,4,9,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	3,7,10,12	2,4,9,15	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	3,7,10,12,16,17,18	2,4,9,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	3,7,10,12,14,17	2,4,9,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	3,7,10,12,14,16,18	2,4,9,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	3,7,10,12,14,17,18	2,4,9,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	3,7,10,12,14,16	2,4,9,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	3,7,10,12	2,4,9,13	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	3,7,10,12,16,17,18	2,4,9,13,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	3,7,10,12,18	2,4,9,13,15,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	3,7,10,12,16,17	2,4,9,13,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	3,7,10,12,14,17,18	2,4,9,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	3,7,10,12,14,16	2,4,9,13	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	3,7,10,12,14,17	2,4,9,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	3,7,10,12,14,16,18	2,4,9,13,15,18	2^{-12}

Table 0.920 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	3,7,10,17,18	2,4,9,11,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	3,7,10,16	2,4,9,11	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,7,10,17	2,4,9,11,15,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	3,7,10,16,18	2,4,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	3,7,10,14	2,4,9,11	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	3,7,10,14,16,17,18	2,4,9,11,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	3,7,10,14,18	2,4,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	3,7,10,14,16,17	2,4,9,11,15,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	3,7,10,17	2,4,9,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	3,7,10,16,18	2,4,9,11,13,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	3,7,10,17,18	2,4,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	3,7,10,16	2,4,9,11,13,15	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	3,7,10,14,18	2,4,9,11,13,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	3,7,10,14,16,17	2,4,9,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	3,7,10,14	2,4,9,11,13,15	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	3,7,10,14,16,17,18	2,4,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	3,7,10,12	2,4,9,11	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	3,7,10,12,16,17,18	2,4,9,11,17,18	2^{-34}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	3,7,10,12,18	2,4,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	3,7,10,12,16,17	2,4,9,11,15,17	2^{-34}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	3,7,10,12,14,17,18	2,4,9,11,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	3,7,10,12,14,16	2,4,9,11	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	3,7,10,12,14,17	2,4,9,11,15,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	3,7,10,12,14,16,18	2,4,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	3,7,10,12,18	2,4,9,11,13,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,7,10,12,16,17	2,4,9,11,13,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	3,7,10,12	2,4,9,11,13,15	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	3,7,10,12,16,17,18	2,4,9,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	3,7,10,12,14,17	2,4,9,11,13,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	3,7,10,12,14,16,18	2,4,9,11,13,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	3,7,10,12,14,17,18	2,4,9,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	3,7,10,12,14,16	2,4,9,11,13,15	2^{-23}

Table 0.921 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	3,7,17,18	2,4,8,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	3,7,16	2,4,8	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	3,7,17	2,4,8,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	3,7,16,18	2,4,8,15,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	3,7,14	2,4,8	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	3,7,14,16,17,18	2,4,8,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	3,7,14,18	2,4,8,15,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	3,7,14,16,17	2,4,8,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	3,7,17	2,4,8,13,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	3,7,16,18	2,4,8,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	3,7,17,18	2,4,8,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	3,7,16	2,4,8,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	3,7,14,18	2,4,8,13,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	3,7,14,16,17	2,4,8,13,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	3,7,14	2,4,8,13,15	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	3,7,14,16,17,18	2,4,8,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	3,7,12	2,4,8	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,7,12,16,17,18	2,4,8,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	3,7,12,18	2,4,8,15,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	3,7,12,16,17	2,4,8,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	3,7,12,14,17,18	2,4,8,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	3,7,12,14,16	2,4,8	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	3,7,12,14,17	2,4,8,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	3,7,12,14,16,18	2,4,8,15,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	3,7,12,18	2,4,8,13,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	3,7,12,16,17	2,4,8,13,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	3,7,12	2,4,8,13,15	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	3,7,12,16,17,18	2,4,8,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	3,7,12,14,17	2,4,8,13,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	3,7,12,14,16,18	2,4,8,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	3,7,12,14,17,18	2,4,8,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	3,7,12,14,16	2,4,8,13,15	$2^{-17.5}$

Table 0.922 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	3,7,17	2,4,8,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	3,7,16,18	2,4,8,11,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	3,7,17,18	2,4,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,7,16	2,4,8,11,15	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	3,7,14,18	2,4,8,11,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	3,7,14,16,17	2,4,8,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	3,7,14	2,4,8,11,15	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	3,7,14,16,17,18	2,4,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	3,7,17,18	2,4,8,11,13,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	3,7,16	2,4,8,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	3,7,17	2,4,8,11,13,15,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	3,7,16,18	2,4,8,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	3,7,14	2,4,8,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	3,7,14,16,17,18	2,4,8,11,13,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	3,7,14,18	2,4,8,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	3,7,14,16,17	2,4,8,11,13,15,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	3,7,12,18	2,4,8,11,18	2^{-34}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	3,7,12,16,17	2,4,8,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	3,7,12	2,4,8,11,15	2^{-34}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	3,7,12,16,17,18	2,4,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	3,7,12,14,17	2,4,8,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	3,7,12,14,16,18	2,4,8,11,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	3,7,12,14,17,18	2,4,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	3,7,12,14,16	2,4,8,11,15	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,7,12	2,4,8,11,13	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	3,7,12,16,17,18	2,4,8,11,13,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	3,7,12,18	2,4,8,11,13,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	3,7,12,16,17	2,4,8,11,13,15,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	3,7,12,14,17,18	2,4,8,11,13,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	3,7,12,14,16	2,4,8,11,13	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	3,7,12,14,17	2,4,8,11,13,15,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	3,7,12,14,16,18	2,4,8,11,13,15,18	$2^{-28.5}$

Table 0.923 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	3,7,10	2,4,8	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	3,7,10,16,17,18	2,4,8,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	3,7,10,18	2,4,8,15,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	3,7,10,16,17	2,4,8,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	3,7,10,14,17,18	2,4,8,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	3,7,10,14,16	2,4,8	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	3,7,10,14,17	2,4,8,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	3,7,10,14,16,18	2,4,8,15,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	3,7,10,18	2,4,8,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	3,7,10,16,17	2,4,8,13,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	3,7,10	2,4,8,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	3,7,10,16,17,18	2,4,8,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	3,7,10,14,17	2,4,8,13,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	3,7,10,14,16,18	2,4,8,13,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	3,7,10,14,17,18	2,4,8,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	3,7,10,14,16	2,4,8,13,15	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	3,7,10,12,17,18	2,4,8,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	3,7,10,12,16	2,4,8	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	3,7,10,12,17	2,4,8,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	3,7,10,12,16,18	2,4,8,15,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	3,7,10,12,14	2,4,8	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	3,7,10,12,14,16,17,18	2,4,8,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	3,7,10,12,14,18	2,4,8,15,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	3,7,10,12,14,16,17	2,4,8,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	3,7,10,12,17	2,4,8,13,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	3,7,10,12,16,18	2,4,8,13,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	3,7,10,12,17,18	2,4,8,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	3,7,10,12,16	2,4,8,13,15	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	3,7,10,12,14,18	2,4,8,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	3,7,10,12,14,16,17	2,4,8,13,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	3,7,10,12,14	2,4,8,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	3,7,10,12,14,16,17,18	2,4,8,13,15,17,18	2^{-23}

Table 0.924 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,7,10,18	2,4,8,11,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	3,7,10,16,17	2,4,8,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	3,7,10	2,4,8,11,15	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	3,7,10,16,17,18	2,4,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	3,7,10,14,17	2,4,8,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	3,7,10,14,16,18	2,4,8,11,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	3,7,10,14,17,18	2,4,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	3,7,10,14,16	2,4,8,11,15	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,7,10	2,4,8,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	3,7,10,16,17,18	2,4,8,11,13,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,7,10,18	2,4,8,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	3,7,10,16,17	2,4,8,11,13,15,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,7,10,14,17,18	2,4,8,11,13,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,7,10,14,16	2,4,8,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	3,7,10,14,17	2,4,8,11,13,15,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,7,10,14,16,18	2,4,8,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	3,7,10,12,17	2,4,8,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	3,7,10,12,16,18	2,4,8,11,18	2^{-1}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	3,7,10,12,17,18	2,4,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,7,10,12,16	2,4,8,11,15	2^{-1}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	3,7,10,12,14,18	2,4,8,11,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	3,7,10,12,14,16,17	2,4,8,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	3,7,10,12,14	2,4,8,11,15	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	3,7,10,12,14,16,17,18	2,4,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	3,7,10,12,17,18	2,4,8,11,13,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	3,7,10,12,16	2,4,8,11,13	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	3,7,10,12,17	2,4,8,11,13,15,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	3,7,10,12,16,18	2,4,8,11,13,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	3,7,10,12,14	2,4,8,11,13	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	3,7,10,12,14,16,17,18	2,4,8,11,13,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	3,7,10,12,14,18	2,4,8,11,13,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	3,7,10,12,14,16,17	2,4,8,11,13,15,17	2^{-12}

Table 0.925 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	3,7,17	2,4,8,9,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,7,16,18	2,4,8,9,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	3,7,17,18	2,4,8,9,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	3,7,16	2,4,8,9,15	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	3,7,14,18	2,4,8,9,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	3,7,14,16,17	2,4,8,9,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	3,7,14	2,4,8,9,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	3,7,14,16,17,18	2,4,8,9,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	3,7,17,18	2,4,8,9,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,7,16	2,4,8,9,13	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	3,7,17	2,4,8,9,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	3,7,16,18	2,4,8,9,13,15,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	3,7,14	2,4,8,9,13	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	3,7,14,16,17,18	2,4,8,9,13,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	3,7,14,18	2,4,8,9,13,15,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	3,7,14,16,17	2,4,8,9,13,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	3,7,12,18	2,4,8,9,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	3,7,12,16,17	2,4,8,9,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	3,7,12	2,4,8,9,15	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	3,7,12,16,17,18	2,4,8,9,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	3,7,12,14,17	2,4,8,9,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	3,7,12,14,16,18	2,4,8,9,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	3,7,12,14,17,18	2,4,8,9,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,7,12,14,16	2,4,8,9,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	3,7,12	2,4,8,9,13	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	3,7,12,16,17,18	2,4,8,9,13,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	3,7,12,18	2,4,8,9,13,15,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	3,7,12,16,17	2,4,8,9,13,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	3,7,12,14,17,18	2,4,8,9,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	3,7,12,14,16	2,4,8,9,13	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	3,7,12,14,17	2,4,8,9,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	3,7,12,14,16,18	2,4,8,9,13,15,18	2^{-23}

Table 0.926 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	3,7,17,18	2,4,8,9,11,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	3,7,16	2,4,8,9,11	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	3,7,17	2,4,8,9,11,15,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	3,7,16,18	2,4,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	3,7,14	2,4,8,9,11	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	3,7,14,16,17,18	2,4,8,9,11,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,7,14,18	2,4,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,7,14,16,17	2,4,8,9,11,15,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	3,7,17	2,4,8,9,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	3,7,16,18	2,4,8,9,11,13,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	3,7,17,18	2,4,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	3,7,16	2,4,8,9,11,13,15	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	3,7,14,18	2,4,8,9,11,13,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	3,7,14,16,17	2,4,8,9,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	3,7,14	2,4,8,9,11,13,15	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	3,7,14,16,17,18	2,4,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	3,7,12	2,4,8,9,11	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	3,7,12,16,17,18	2,4,8,9,11,17,18	2^{-1}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	3,7,12,18	2,4,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	3,7,12,16,17	2,4,8,9,11,15,17	2^{-1}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	3,7,12,14,17,18	2,4,8,9,11,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	3,7,12,14,16	2,4,8,9,11	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	3,7,12,14,17	2,4,8,9,11,15,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	3,7,12,14,16,18	2,4,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	3,7,12,18	2,4,8,9,11,13,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	3,7,12,16,17	2,4,8,9,11,13,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	3,7,12	2,4,8,9,11,13,15	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	3,7,12,16,17,18	2,4,8,9,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	3,7,12,14,17	2,4,8,9,11,13,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,7,12,14,16,18	2,4,8,9,11,13,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	3,7,12,14,17,18	2,4,8,9,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	3,7,12,14,16	2,4,8,9,11,13,15	2^{-12}

Table 0.927 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	3,7,10,18	2,4,8,9,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	3,7,10,16,17	2,4,8,9,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	3,7,10	2,4,8,9,15	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	3,7,10,16,17,18	2,4,8,9,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	3,7,10,14,17	2,4,8,9,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	3,7,10,14,16,18	2,4,8,9,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	3,7,10,14,17,18	2,4,8,9,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	3,7,10,14,16	2,4,8,9,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	3,7,10	2,4,8,9,13	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,7,10,16,17,18	2,4,8,9,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	3,7,10,18	2,4,8,9,13,15,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	3,7,10,16,17	2,4,8,9,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	3,7,10,14,17,18	2,4,8,9,13,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	3,7,10,14,16	2,4,8,9,13	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	3,7,10,14,17	2,4,8,9,13,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	3,7,10,14,16,18	2,4,8,9,13,15,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	3,7,10,12,17	2,4,8,9,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	3,7,10,12,16,18	2,4,8,9,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	3,7,10,12,17,18	2,4,8,9,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	3,7,10,12,16	2,4,8,9,15	$2^{-6.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	3,7,10,12,14,18	2,4,8,9,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	3,7,10,12,14,16,17	2,4,8,9,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	3,7,10,12,14	2,4,8,9,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	3,7,10,12,14,16,17,18	2,4,8,9,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	3,7,10,12,17,18	2,4,8,9,13,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	3,7,10,12,16	2,4,8,9,13	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	3,7,10,12,17	2,4,8,9,13,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	3,7,10,12,16,18	2,4,8,9,13,15,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	3,7,10,12,14	2,4,8,9,13	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	3,7,10,12,14,16,17,18	2,4,8,9,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	3,7,10,12,14,18	2,4,8,9,13,15,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	3,7,10,12,14,16,17	2,4,8,9,13,15,17	$2^{-17.5}$

Table 0.928 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	3,7,10	2,4,8,9,11	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	3,7,10,16,17,18	2,4,8,9,11,17,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	3,7,10,18	2,4,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	3,7,10,16,17	2,4,8,9,11,15,17	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	3,7,10,14,17,18	2,4,8,9,11,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	3,7,10,14,16	2,4,8,9,11	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	3,7,10,14,17	2,4,8,9,11,15,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	3,7,10,14,16,18	2,4,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	3,7,10,18	2,4,8,9,11,13,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	3,7,10,16,17	2,4,8,9,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	3,7,10	2,4,8,9,11,13,15	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	3,7,10,16,17,18	2,4,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	3,7,10,14,17	2,4,8,9,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	3,7,10,14,16,18	2,4,8,9,11,13,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	3,7,10,14,17,18	2,4,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	3,7,10,14,16	2,4,8,9,11,13,15	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	3,7,10,12,17,18	2,4,8,9,11,17,18	2^{-34}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	3,7,10,12,16	2,4,8,9,11	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	3,7,10,12,17	2,4,8,9,11,15,17	2^{-34}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	3,7,10,12,16,18	2,4,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	3,7,10,12,14	2,4,8,9,11	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	3,7,10,12,14,16,17,18	2,4,8,9,11,17,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	3,7,10,12,14,18	2,4,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	3,7,10,12,14,16,17	2,4,8,9,11,15,17	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	3,7,10,12,17	2,4,8,9,11,13,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	3,7,10,12,16,18	2,4,8,9,11,13,18	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	3,7,10,12,17,18	2,4,8,9,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	3,7,10,12,16	2,4,8,9,11,13,15	2^{-12}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	3,7,10,12,14,18	2,4,8,9,11,13,18	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	3,7,10,12,14,16,17	2,4,8,9,11,13,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	3,7,10,12,14	2,4,8,9,11,13,15	2^{-23}
$(0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	3,7,10,12,14,16,17,18	2,4,8,9,11,13,15,17,18	$2^{-28.5}$

Table 0.929 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	3,17	2,4,6,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	3,16,18	2,4,6,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	3,17,18	2,4,6,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	3,16	2,4,6,15	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	3,14,18	2,4,6,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	3,14,16,17	2,4,6,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	3,14	2,4,6,15	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	3,14,16,17,18	2,4,6,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	3,17,18	2,4,6,13,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	3,16	2,4,6,13	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	3,17	2,4,6,13,15,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	3,16,18	2,4,6,13,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	3,14	2,4,6,13	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	3,14,16,17,18	2,4,6,13,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,14,18	2,4,6,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,14,16,17	2,4,6,13,15,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	3,12,18	2,4,6,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	3,12,16,17	2,4,6,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	3,12	2,4,6,15	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	3,12,16,17,18	2,4,6,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,12,14,17	2,4,6,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	3,12,14,16,18	2,4,6,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	3,12,14,17,18	2,4,6,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	3,12,14,16	2,4,6,15	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	3,12	2,4,6,13	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	3,12,16,17,18	2,4,6,13,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	3,12,18	2,4,6,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	3,12,16,17	2,4,6,13,15,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	3,12,14,17,18	2,4,6,13,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	3,12,14,16	2,4,6,13	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	3,12,14,17	2,4,6,13,15,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	3,12,14,16,18	2,4,6,13,15,18	$2^{-28.5}$

Table 0.930 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	3,17,18	2,4,6,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	3,16	2,4,6,11	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	3,17	2,4,6,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	3,16,18	2,4,6,11,15,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	3,14	2,4,6,11	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	3,14,16,17,18	2,4,6,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,14,18	2,4,6,11,15,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	3,14,16,17	2,4,6,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	3,17	2,4,6,11,13,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	3,16,18	2,4,6,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	3,17,18	2,4,6,11,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	3,16	2,4,6,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	3,14,18	2,4,6,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	3,14,16,17	2,4,6,11,13,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	3,14	2,4,6,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	3,14,16,17,18	2,4,6,11,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	3,12	2,4,6,11	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	3,12,16,17,18	2,4,6,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	3,12,18	2,4,6,11,15,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	3,12,16,17	2,4,6,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	3,12,14,17,18	2,4,6,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	3,12,14,16	2,4,6,11	2^{-34}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	3,12,14,17	2,4,6,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	3,12,14,16,18	2,4,6,11,15,18	2^{-34}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	3,12,18	2,4,6,11,13,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	3,12,16,17	2,4,6,11,13,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	3,12	2,4,6,11,13,15	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	3,12,16,17,18	2,4,6,11,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	3,12,14,17	2,4,6,11,13,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	3,12,14,16,18	2,4,6,11,13,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	3,12,14,17,18	2,4,6,11,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	3,12,14,16	2,4,6,11,13,15	$2^{-28.5}$

Table 0.931 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	3,10,18	2,4,6,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	3,10,16,17	2,4,6,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	3,10	2,4,6,15	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	3,10,16,17,18	2,4,6,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,10,14,17	2,4,6,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	3,10,14,16,18	2,4,6,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	3,10,14,17,18	2,4,6,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	3,10,14,16	2,4,6,15	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	3,10	2,4,6,13	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	3,10,16,17,18	2,4,6,13,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	3,10,18	2,4,6,13,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	3,10,16,17	2,4,6,13,15,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	3,10,14,17,18	2,4,6,13,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	3,10,14,16	2,4,6,13	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	3,10,14,17	2,4,6,13,15,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	3,10,14,16,18	2,4,6,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	3,10,12,17	2,4,6,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	3,10,12,16,18	2,4,6,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	3,10,12,17,18	2,4,6,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	3,10,12,16	2,4,6,15	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	3,10,12,14,18	2,4,6,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	3,10,12,14,16,17	2,4,6,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	3,10,12,14	2,4,6,15	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,10,12,14,16,17,18	2,4,6,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	3,10,12,17,18	2,4,6,13,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	3,10,12,16	2,4,6,13	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	3,10,12,17	2,4,6,13,15,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	3,10,12,16,18	2,4,6,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	3,10,12,14	2,4,6,13	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	3,10,12,14,16,17,18	2,4,6,13,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	3,10,12,14,18	2,4,6,13,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,10,12,14,16,17	2,4,6,13,15,17	2^{-23}

Table 0.932 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	3,10	2,4,6,11	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	3,10,16,17,18	2,4,6,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	3,10,18	2,4,6,11,15,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	3,10,16,17	2,4,6,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	3,10,14,17,18	2,4,6,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	3,10,14,16	2,4,6,11	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	3,10,14,17	2,4,6,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	3,10,14,16,18	2,4,6,11,15,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	3,10,18	2,4,6,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	3,10,16,17	2,4,6,11,13,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	3,10	2,4,6,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	3,10,16,17,18	2,4,6,11,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	3,10,14,17	2,4,6,11,13,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	3,10,14,16,18	2,4,6,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	3,10,14,17,18	2,4,6,11,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	3,10,14,16	2,4,6,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	3,10,12,17,18	2,4,6,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	3,10,12,16	2,4,6,11	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	3,10,12,17	2,4,6,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	3,10,12,16,18	2,4,6,11,15,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	3,10,12,14	2,4,6,11	2^{-1}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	3,10,12,14,16,17,18	2,4,6,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	3,10,12,14,18	2,4,6,11,15,18	2^{-1}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	3,10,12,14,16,17	2,4,6,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	3,10,12,17	2,4,6,11,13,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	3,10,12,16,18	2,4,6,11,13,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	3,10,12,17,18	2,4,6,11,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	3,10,12,16	2,4,6,11,13,15	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	3,10,12,14,18	2,4,6,11,13,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	3,10,12,14,16,17	2,4,6,11,13,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	3,10,12,14	2,4,6,11,13,15	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	3,10,12,14,16,17,18	2,4,6,11,13,15,17,18	2^{-23}

Table 0.933 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	3,17,18	2,4,6,9,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	3,16	2,4,6,9	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	3,17	2,4,6,9,15,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	3,16,18	2,4,6,9,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	3,14	2,4,6,9	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	3,14,16,17,18	2,4,6,9,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	3,14,18	2,4,6,9,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	3,14,16,17	2,4,6,9,15,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	3,17	2,4,6,9,13,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	3,16,18	2,4,6,9,13,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,17,18	2,4,6,9,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	3,16	2,4,6,9,13,15	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	3,14,18	2,4,6,9,13,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	3,14,16,17	2,4,6,9,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	3,14	2,4,6,9,13,15	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	3,14,16,17,18	2,4,6,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,12	2,4,6,9	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,12,16,17,18	2,4,6,9,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	3,12,18	2,4,6,9,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	3,12,16,17	2,4,6,9,15,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	3,12,14,17,18	2,4,6,9,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	3,12,14,16	2,4,6,9	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	3,12,14,17	2,4,6,9,15,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	3,12,14,16,18	2,4,6,9,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	3,12,18	2,4,6,9,13,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	3,12,16,17	2,4,6,9,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	3,12	2,4,6,9,13,15	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	3,12,16,17,18	2,4,6,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	3,12,14,17	2,4,6,9,13,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	3,12,14,16,18	2,4,6,9,13,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	3,12,14,17,18	2,4,6,9,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	3,12,14,16	2,4,6,9,13,15	2^{-23}

Table 0.934 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,17	2,4,6,9,11,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	3,16,18	2,4,6,9,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	3,17,18	2,4,6,9,11,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	3,16	2,4,6,9,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	3,14,18	2,4,6,9,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	3,14,16,17	2,4,6,9,11,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	3,14	2,4,6,9,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	3,14,16,17,18	2,4,6,9,11,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	3,17,18	2,4,6,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	3,16	2,4,6,9,11,13	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	3,17	2,4,6,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	3,16,18	2,4,6,9,11,13,15,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	3,14	2,4,6,9,11,13	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	3,14,16,17,18	2,4,6,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	3,14,18	2,4,6,9,11,13,15,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	3,14,16,17	2,4,6,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	3,12,18	2,4,6,9,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	3,12,16,17	2,4,6,9,11,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	3,12	2,4,6,9,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	3,12,16,17,18	2,4,6,9,11,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	3,12,14,17	2,4,6,9,11,17	2^{-1}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	3,12,14,16,18	2,4,6,9,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,12,14,17,18	2,4,6,9,11,15,17,18	2^{-1}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	3,12,14,16	2,4,6,9,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	3,12	2,4,6,9,11,13	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	3,12,16,17,18	2,4,6,9,11,13,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	3,12,18	2,4,6,9,11,13,15,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	3,12,16,17	2,4,6,9,11,13,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	3,12,14,17,18	2,4,6,9,11,13,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	3,12,14,16	2,4,6,9,11,13	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,12,14,17	2,4,6,9,11,13,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	3,12,14,16,18	2,4,6,9,11,13,15,18	2^{-23}

Table 0.935 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	3,10	2,4,6,9	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	3,10,16,17,18	2,4,6,9,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	3,10,18	2,4,6,9,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	3,10,16,17	2,4,6,9,15,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	3,10,14,17,18	2,4,6,9,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	3,10,14,16	2,4,6,9	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	3,10,14,17	2,4,6,9,15,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	3,10,14,16,18	2,4,6,9,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	3,10,18	2,4,6,9,13,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	3,10,16,17	2,4,6,9,13,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	3,10	2,4,6,9,13,15	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	3,10,16,17,18	2,4,6,9,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	3,10,14,17	2,4,6,9,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	3,10,14,16,18	2,4,6,9,13,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,10,14,17,18	2,4,6,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	3,10,14,16	2,4,6,9,13,15	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	3,10,12,17,18	2,4,6,9,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	3,10,12,16	2,4,6,9	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	3,10,12,17	2,4,6,9,15,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	3,10,12,16,18	2,4,6,9,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	3,10,12,14	2,4,6,9	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	3,10,12,14,16,17,18	2,4,6,9,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	3,10,12,14,18	2,4,6,9,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	3,10,12,14,16,17	2,4,6,9,15,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	3,10,12,17	2,4,6,9,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	3,10,12,16,18	2,4,6,9,13,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	3,10,12,17,18	2,4,6,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	3,10,12,16	2,4,6,9,13,15	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	3,10,12,14,18	2,4,6,9,13,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	3,10,12,14,16,17	2,4,6,9,13,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	3,10,12,14	2,4,6,9,13,15	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	3,10,12,14,16,17,18	2,4,6,9,13,15,17,18	$2^{-28.5}$

Table 0.936 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	3,10,18	2,4,6,9,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	3,10,16,17	2,4,6,9,11,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	3,10	2,4,6,9,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	3,10,16,17,18	2,4,6,9,11,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	3,10,14,17	2,4,6,9,11,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	3,10,14,16,18	2,4,6,9,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	3,10,14,17,18	2,4,6,9,11,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	3,10,14,16	2,4,6,9,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	3,10	2,4,6,9,11,13	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	3,10,16,17,18	2,4,6,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	3,10,18	2,4,6,9,11,13,15,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	3,10,16,17	2,4,6,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	3,10,14,17,18	2,4,6,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	3,10,14,16	2,4,6,9,11,13	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	3,10,14,17	2,4,6,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	3,10,14,16,18	2,4,6,9,11,13,15,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	3,10,12,17	2,4,6,9,11,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	3,10,12,16,18	2,4,6,9,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	3,10,12,17,18	2,4,6,9,11,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	3,10,12,16	2,4,6,9,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	3,10,12,14,18	2,4,6,9,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	3,10,12,14,16,17	2,4,6,9,11,17	2^{-34}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	3,10,12,14	2,4,6,9,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	3,10,12,14,16,17,18	2,4,6,9,11,15,17,18	2^{-34}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	3,10,12,17,18	2,4,6,9,11,13,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	3,10,12,16	2,4,6,9,11,13	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	3,10,12,17	2,4,6,9,11,13,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	3,10,12,16,18	2,4,6,9,11,13,15,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	3,10,12,14	2,4,6,9,11,13	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	3,10,12,14,16,17,18	2,4,6,9,11,13,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,10,12,14,18	2,4,6,9,11,13,15,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	3,10,12,14,16,17	2,4,6,9,11,13,15,17	$2^{-28.5}$

Table 0.937 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	3,18	2,4,6,8,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	3,16,17	2,4,6,8,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	3	2,4,6,8,15	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	3,16,17,18	2,4,6,8,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	3,14,17	2,4,6,8,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	3,14,16,18	2,4,6,8,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	3,14,17,18	2,4,6,8,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	3,14,16	2,4,6,8,15	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	3	2,4,6,8,13	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	3,16,17,18	2,4,6,8,13,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	3,18	2,4,6,8,13,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	3,16,17	2,4,6,8,13,15,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	3,14,17,18	2,4,6,8,13,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	3,14,16	2,4,6,8,13	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	3,14,17	2,4,6,8,13,15,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	3,14,16,18	2,4,6,8,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	3,12,17	2,4,6,8,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	3,12,16,18	2,4,6,8,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	3,12,17,18	2,4,6,8,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	3,12,16	2,4,6,8,15	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	3,12,14,18	2,4,6,8,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	3,12,14,16,17	2,4,6,8,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	3,12,14	2,4,6,8,15	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	3,12,14,16,17,18	2,4,6,8,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	3,12,17,18	2,4,6,8,13,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	3,12,16	2,4,6,8,13	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	3,12,17	2,4,6,8,13,15,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	3,12,16,18	2,4,6,8,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	3,12,14	2,4,6,8,13	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	3,12,14,16,17,18	2,4,6,8,13,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	3,12,14,18	2,4,6,8,13,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	3,12,14,16,17	2,4,6,8,13,15,17	2^{-12}

Table 0.938 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	3	2,4,6,8,11	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	3,16,17,18	2,4,6,8,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	3,18	2,4,6,8,11,15,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	3,16,17	2,4,6,8,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	3,14,17,18	2,4,6,8,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	3,14,16	2,4,6,8,11	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	3,14,17	2,4,6,8,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	3,14,16,18	2,4,6,8,11,15,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	3,18	2,4,6,8,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	3,16,17	2,4,6,8,11,13,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	3	2,4,6,8,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	3,16,17,18	2,4,6,8,11,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	3,14,17	2,4,6,8,11,13,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	3,14,16,18	2,4,6,8,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	3,14,17,18	2,4,6,8,11,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	3,14,16	2,4,6,8,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	3,12,17,18	2,4,6,8,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	3,12,16	2,4,6,8,11	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	3,12,17	2,4,6,8,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	3,12,16,18	2,4,6,8,11,15,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	3,12,14	2,4,6,8,11	2^{-34}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	3,12,14,16,17,18	2,4,6,8,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	3,12,14,18	2,4,6,8,11,15,18	2^{-34}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	3,12,14,16,17	2,4,6,8,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	3,12,17	2,4,6,8,11,13,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	3,12,16,18	2,4,6,8,11,13,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	3,12,17,18	2,4,6,8,11,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	3,12,16	2,4,6,8,11,13,15	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	3,12,14,18	2,4,6,8,11,13,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	3,12,14,16,17	2,4,6,8,11,13,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	3,12,14	2,4,6,8,11,13,15	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,12,14,16,17,18	2,4,6,8,11,13,15,17,18	2^{-12}

Table 0.939 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	3,10,17	2,4,6,8,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	3,10,16,18	2,4,6,8,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	3,10,17,18	2,4,6,8,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	3,10,16	2,4,6,8,15	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	3,10,14,18	2,4,6,8,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	3,10,14,16,17	2,4,6,8,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	3,10,14	2,4,6,8,15	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	3,10,14,16,17,18	2,4,6,8,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	3,10,17,18	2,4,6,8,13,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	3,10,16	2,4,6,8,13	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	3,10,17	2,4,6,8,13,15,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,10,16,18	2,4,6,8,13,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	3,10,14	2,4,6,8,13	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	3,10,14,16,17,18	2,4,6,8,13,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	3,10,14,18	2,4,6,8,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	3,10,14,16,17	2,4,6,8,13,15,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,10,12,18	2,4,6,8,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,10,12,16,17	2,4,6,8,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	3,10,12	2,4,6,8,15	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	3,10,12,16,17,18	2,4,6,8,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	3,10,12,14,17	2,4,6,8,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	3,10,12,14,16,18	2,4,6,8,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	3,10,12,14,17,18	2,4,6,8,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	3,10,12,14,16	2,4,6,8,15	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	3,10,12	2,4,6,8,13	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	3,10,12,16,17,18	2,4,6,8,13,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	3,10,12,18	2,4,6,8,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	3,10,12,16,17	2,4,6,8,13,15,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	3,10,12,14,17,18	2,4,6,8,13,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	3,10,12,14,16	2,4,6,8,13	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	3,10,12,14,17	2,4,6,8,13,15,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	3,10,12,14,16,18	2,4,6,8,13,15,18	$2^{-6.5}$

Table 0.940 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	3,10,17,18	2,4,6,8,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,10,16	2,4,6,8,11	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	3,10,17	2,4,6,8,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	3,10,16,18	2,4,6,8,11,15,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	3,10,14	2,4,6,8,11	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	3,10,14,16,17,18	2,4,6,8,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	3,10,14,18	2,4,6,8,11,15,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	3,10,14,16,17	2,4,6,8,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	3,10,17	2,4,6,8,11,13,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	3,10,16,18	2,4,6,8,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	3,10,17,18	2,4,6,8,11,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	3,10,16	2,4,6,8,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	3,10,14,18	2,4,6,8,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	3,10,14,16,17	2,4,6,8,11,13,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	3,10,14	2,4,6,8,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	3,10,14,16,17,18	2,4,6,8,11,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	3,10,12	2,4,6,8,11	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	3,10,12,16,17,18	2,4,6,8,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	3,10,12,18	2,4,6,8,11,15,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	3,10,12,16,17	2,4,6,8,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	3,10,12,14,17,18	2,4,6,8,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	3,10,12,14,16	2,4,6,8,11	2^{-1}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	3,10,12,14,17	2,4,6,8,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,10,12,14,16,18	2,4,6,8,11,15,18	2^{-1}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	3,10,12,18	2,4,6,8,11,13,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	3,10,12,16,17	2,4,6,8,11,13,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	3,10,12	2,4,6,8,11,13,15	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	3,10,12,16,17,18	2,4,6,8,11,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	3,10,12,14,17	2,4,6,8,11,13,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	3,10,12,14,16,18	2,4,6,8,11,13,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	3,10,12,14,17,18	2,4,6,8,11,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,10,12,14,16	2,4,6,8,11,13,15	$2^{-6.5}$

Table 0.941 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	3	2,4,6,8,9	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	3,16,17,18	2,4,6,8,9,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	3,18	2,4,6,8,9,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	3,16,17	2,4,6,8,9,15,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	3,14,17,18	2,4,6,8,9,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,14,16	2,4,6,8,9	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	3,14,17	2,4,6,8,9,15,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	3,14,16,18	2,4,6,8,9,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	3,18	2,4,6,8,9,13,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	3,16,17	2,4,6,8,9,13,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	3	2,4,6,8,9,13,15	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	3,16,17,18	2,4,6,8,9,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	3,14,17	2,4,6,8,9,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	3,14,16,18	2,4,6,8,9,13,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	3,14,17,18	2,4,6,8,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	3,14,16	2,4,6,8,9,13,15	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	3,12,17,18	2,4,6,8,9,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	3,12,16	2,4,6,8,9	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	3,12,17	2,4,6,8,9,15,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	3,12,16,18	2,4,6,8,9,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	3,12,14	2,4,6,8,9	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	3,12,14,16,17,18	2,4,6,8,9,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,12,14,18	2,4,6,8,9,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	3,12,14,16,17	2,4,6,8,9,15,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	3,12,17	2,4,6,8,9,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	3,12,16,18	2,4,6,8,9,13,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	3,12,17,18	2,4,6,8,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	3,12,16	2,4,6,8,9,13,15	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	3,12,14,18	2,4,6,8,9,13,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	3,12,14,16,17	2,4,6,8,9,13,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,12,14	2,4,6,8,9,13,15	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	3,12,14,16,17,18	2,4,6,8,9,13,15,17,18	$2^{-6.5}$

Table 0.942 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	3,18	2,4,6,8,9,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	3,16,17	2,4,6,8,9,11,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	3	2,4,6,8,9,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	3,16,17,18	2,4,6,8,9,11,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	3,14,17	2,4,6,8,9,11,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	3,14,16,18	2,4,6,8,9,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	3,14,17,18	2,4,6,8,9,11,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	3,14,16	2,4,6,8,9,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	3	2,4,6,8,9,11,13	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	3,16,17,18	2,4,6,8,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	3,18	2,4,6,8,9,11,13,15,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	3,16,17	2,4,6,8,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	3,14,17,18	2,4,6,8,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,14,16	2,4,6,8,9,11,13	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	3,14,17	2,4,6,8,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	3,14,16,18	2,4,6,8,9,11,13,15,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	3,12,17	2,4,6,8,9,11,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	3,12,16,18	2,4,6,8,9,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	3,12,17,18	2,4,6,8,9,11,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	3,12,16	2,4,6,8,9,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	3,12,14,18	2,4,6,8,9,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	3,12,14,16,17	2,4,6,8,9,11,17	2^{-1}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	3,12,14	2,4,6,8,9,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	3,12,14,16,17,18	2,4,6,8,9,11,15,17,18	2^{-1}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	3,12,17,18	2,4,6,8,9,11,13,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	3,12,16	2,4,6,8,9,11,13	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	3,12,17	2,4,6,8,9,11,13,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	3,12,16,18	2,4,6,8,9,11,13,15,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	3,12,14	2,4,6,8,9,11,13	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	3,12,14,16,17,18	2,4,6,8,9,11,13,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	3,12,14,18	2,4,6,8,9,11,13,15,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	3,12,14,16,17	2,4,6,8,9,11,13,15,17	$2^{-6.5}$

Table 0.943 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	3,10,17,18	2,4,6,8,9,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	3,10,16	2,4,6,8,9	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	3,10,17	2,4,6,8,9,15,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	3,10,16,18	2,4,6,8,9,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	3,10,14	2,4,6,8,9	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	3,10,14,16,17,18	2,4,6,8,9,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	3,10,14,18	2,4,6,8,9,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	3,10,14,16,17	2,4,6,8,9,15,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	3,10,17	2,4,6,8,9,13,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	3,10,16,18	2,4,6,8,9,13,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	3,10,17,18	2,4,6,8,9,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	3,10,16	2,4,6,8,9,13,15	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	3,10,14,18	2,4,6,8,9,13,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	3,10,14,16,17	2,4,6,8,9,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,10,14	2,4,6,8,9,13,15	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,10,14,16,17,18	2,4,6,8,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	3,10,12	2,4,6,8,9	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	3,10,12,16,17,18	2,4,6,8,9,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	3,10,12,18	2,4,6,8,9,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	3,10,12,16,17	2,4,6,8,9,15,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	3,10,12,14,17,18	2,4,6,8,9,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,10,12,14,16	2,4,6,8,9	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	3,10,12,14,17	2,4,6,8,9,15,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	3,10,12,14,16,18	2,4,6,8,9,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	3,10,12,18	2,4,6,8,9,13,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	3,10,12,16,17	2,4,6,8,9,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	3,10,12	2,4,6,8,9,13,15	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	3,10,12,16,17,18	2,4,6,8,9,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	3,10,12,14,17	2,4,6,8,9,13,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	3,10,12,14,16,18	2,4,6,8,9,13,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	3,10,12,14,17,18	2,4,6,8,9,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	3,10,12,14,16	2,4,6,8,9,13,15	2^{-12}

Table 0.944 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	3,10,17	2,4,6,8,9,11,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	3,10,16,18	2,4,6,8,9,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	3,10,17,18	2,4,6,8,9,11,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	3,10,16	2,4,6,8,9,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	3,10,14,18	2,4,6,8,9,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	3,10,14,16,17	2,4,6,8,9,11,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	3,10,14	2,4,6,8,9,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,10,14,16,17,18	2,4,6,8,9,11,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	3,10,17,18	2,4,6,8,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	3,10,16	2,4,6,8,9,11,13	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	3,10,17	2,4,6,8,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	3,10,16,18	2,4,6,8,9,11,13,15,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	3,10,14	2,4,6,8,9,11,13	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	3,10,14,16,17,18	2,4,6,8,9,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	3,10,14,18	2,4,6,8,9,11,13,15,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	3,10,14,16,17	2,4,6,8,9,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	3,10,12,18	2,4,6,8,9,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	3,10,12,16,17	2,4,6,8,9,11,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	3,10,12	2,4,6,8,9,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	3,10,12,16,17,18	2,4,6,8,9,11,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	3,10,12,14,17	2,4,6,8,9,11,17	2^{-34}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	3,10,12,14,16,18	2,4,6,8,9,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	3,10,12,14,17,18	2,4,6,8,9,11,15,17,18	2^{-34}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	3,10,12,14,16	2,4,6,8,9,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	3,10,12	2,4,6,8,9,11,13	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	3,10,12,16,17,18	2,4,6,8,9,11,13,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	3,10,12,18	2,4,6,8,9,11,13,15,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	3,10,12,16,17	2,4,6,8,9,11,13,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	3,10,12,14,17,18	2,4,6,8,9,11,13,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	3,10,12,14,16	2,4,6,8,9,11,13	2^{-12}
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	3,10,12,14,17	2,4,6,8,9,11,13,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	3,10,12,14,16,18	2,4,6,8,9,11,13,15,18	2^{-12}

Table 0.945 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	3,7,17,18	2,4,6,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	3,7,16	2,4,6	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,7,17	2,4,6,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	3,7,16,18	2,4,6,15,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	3,7,14	2,4,6	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	3,7,14,16,17,18	2,4,6,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	3,7,14,18	2,4,6,15,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	3,7,14,16,17	2,4,6,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	3,7,17	2,4,6,13,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	3,7,16,18	2,4,6,13,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	3,7,17,18	2,4,6,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	3,7,16	2,4,6,13,15	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	3,7,14,18	2,4,6,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	3,7,14,16,17	2,4,6,13,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	3,7,14	2,4,6,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	3,7,14,16,17,18	2,4,6,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	3,7,12	2,4,6	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	3,7,12,16,17,18	2,4,6,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	3,7,12,18	2,4,6,15,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	3,7,12,16,17	2,4,6,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,7,12,14,17,18	2,4,6,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	3,7,12,14,16	2,4,6	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	3,7,12,14,17	2,4,6,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	3,7,12,14,16,18	2,4,6,15,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	3,7,12,18	2,4,6,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	3,7,12,16,17	2,4,6,13,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	3,7,12	2,4,6,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	3,7,12,16,17,18	2,4,6,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,7,12,14,17	2,4,6,13,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	3,7,12,14,16,18	2,4,6,13,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	3,7,12,14,17,18	2,4,6,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	3,7,12,14,16	2,4,6,13,15	$2^{-28.5}$

Table 0.946 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	3,7,17	2,4,6,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	3,7,16,18	2,4,6,11,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	3,7,17,18	2,4,6,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	3,7,16	2,4,6,11,15	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	3,7,14,18	2,4,6,11,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	3,7,14,16,17	2,4,6,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	3,7,14	2,4,6,11,15	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	3,7,14,16,17,18	2,4,6,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,7,17,18	2,4,6,11,13,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	3,7,16	2,4,6,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	3,7,17	2,4,6,11,13,15,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	3,7,16,18	2,4,6,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	3,7,14	2,4,6,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	3,7,14,16,17,18	2,4,6,11,13,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	3,7,14,18	2,4,6,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	3,7,14,16,17	2,4,6,11,13,15,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	3,7,12,18	2,4,6,11,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	3,7,12,16,17	2,4,6,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,7,12	2,4,6,11,15	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,7,12,16,17,18	2,4,6,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	3,7,12,14,17	2,4,6,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	3,7,12,14,16,18	2,4,6,11,18	2^{-34}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	3,7,12,14,17,18	2,4,6,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	3,7,12,14,16	2,4,6,11,15	2^{-34}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	3,7,12	2,4,6,11,13	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	3,7,12,16,17,18	2,4,6,11,13,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	3,7,12,18	2,4,6,11,13,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	3,7,12,16,17	2,4,6,11,13,15,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	3,7,12,14,17,18	2,4,6,11,13,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	3,7,12,14,16	2,4,6,11,13	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	3,7,12,14,17	2,4,6,11,13,15,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	3,7,12,14,16,18	2,4,6,11,13,15,18	$2^{-28.5}$

Table 0.947 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	3,7,10	2,4,6	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	3,7,10,16,17,18	2,4,6,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	3,7,10,18	2,4,6,15,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	3,7,10,16,17	2,4,6,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	3,7,10,14,17,18	2,4,6,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	3,7,10,14,16	2,4,6	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	3,7,10,14,17	2,4,6,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	3,7,10,14,16,18	2,4,6,15,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	3,7,10,18	2,4,6,13,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	3,7,10,16,17	2,4,6,13,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	3,7,10	2,4,6,13,15	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	3,7,10,16,17,18	2,4,6,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	3,7,10,14,17	2,4,6,13,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	3,7,10,14,16,18	2,4,6,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	3,7,10,14,17,18	2,4,6,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	3,7,10,14,16	2,4,6,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	3,7,10,12,17,18	2,4,6,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	3,7,10,12,16	2,4,6	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	3,7,10,12,17	2,4,6,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	3,7,10,12,16,18	2,4,6,15,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	3,7,10,12,14	2,4,6	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	3,7,10,12,14,16,17,18	2,4,6,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	3,7,10,12,14,18	2,4,6,15,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	3,7,10,12,14,16,17	2,4,6,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	3,7,10,12,17	2,4,6,13,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	3,7,10,12,16,18	2,4,6,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	3,7,10,12,17,18	2,4,6,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	3,7,10,12,16	2,4,6,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,7,10,12,14,18	2,4,6,13,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	3,7,10,12,14,16,17	2,4,6,13,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	3,7,10,12,14	2,4,6,13,15	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	3,7,10,12,14,16,17,18	2,4,6,13,15,17,18	2^{-23}

Table 0.948 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	3,7,10,18	2,4,6,11,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	3,7,10,16,17	2,4,6,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	3,7,10	2,4,6,11,15	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	3,7,10,16,17,18	2,4,6,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	3,7,10,14,17	2,4,6,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	3,7,10,14,16,18	2,4,6,11,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	3,7,10,14,17,18	2,4,6,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	3,7,10,14,16	2,4,6,11,15	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	3,7,10	2,4,6,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	3,7,10,16,17,18	2,4,6,11,13,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	3,7,10,18	2,4,6,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	3,7,10,16,17	2,4,6,11,13,15,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	3,7,10,14,17,18	2,4,6,11,13,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	3,7,10,14,16	2,4,6,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	3,7,10,14,17	2,4,6,11,13,15,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	3,7,10,14,16,18	2,4,6,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	3,7,10,12,17	2,4,6,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	3,7,10,12,16,18	2,4,6,11,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	3,7,10,12,17,18	2,4,6,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	3,7,10,12,16	2,4,6,11,15	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	3,7,10,12,14,18	2,4,6,11,18	2^{-1}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	3,7,10,12,14,16,17	2,4,6,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	3,7,10,12,14	2,4,6,11,15	2^{-1}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	3,7,10,12,14,16,17,18	2,4,6,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	3,7,10,12,17,18	2,4,6,11,13,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	3,7,10,12,16	2,4,6,11,13	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	3,7,10,12,17	2,4,6,11,13,15,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	3,7,10,12,16,18	2,4,6,11,13,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	3,7,10,12,14	2,4,6,11,13	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	3,7,10,12,14,16,17,18	2,4,6,11,13,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	3,7,10,12,14,18	2,4,6,11,13,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	3,7,10,12,14,16,17	2,4,6,11,13,15,17	2^{-23}

Table 0.949 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	3,7,17	2,4,6,9,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	3,7,16,18	2,4,6,9,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	3,7,17,18	2,4,6,9,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	3,7,16	2,4,6,9,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,7,14,18	2,4,6,9,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	3,7,14,16,17	2,4,6,9,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	3,7,14	2,4,6,9,15	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	3,7,14,16,17,18	2,4,6,9,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	3,7,17,18	2,4,6,9,13,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	3,7,16	2,4,6,9,13	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	3,7,17	2,4,6,9,13,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	3,7,16,18	2,4,6,9,13,15,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	3,7,14	2,4,6,9,13	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	3,7,14,16,17,18	2,4,6,9,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	3,7,14,18	2,4,6,9,13,15,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	3,7,14,16,17	2,4,6,9,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	3,7,12,18	2,4,6,9,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	3,7,12,16,17	2,4,6,9,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	3,7,12	2,4,6,9,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	3,7,12,16,17,18	2,4,6,9,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	3,7,12,14,17	2,4,6,9,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	3,7,12,14,16,18	2,4,6,9,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	3,7,12,14,17,18	2,4,6,9,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	3,7,12,14,16	2,4,6,9,15	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	3,7,12	2,4,6,9,13	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	3,7,12,16,17,18	2,4,6,9,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	3,7,12,18	2,4,6,9,13,15,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	3,7,12,16,17	2,4,6,9,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	3,7,12,14,17,18	2,4,6,9,13,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	3,7,12,14,16	2,4,6,9,13	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	3,7,12,14,17	2,4,6,9,13,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	3,7,12,14,16,18	2,4,6,9,13,15,18	2^{-23}

Table 0.950 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	3,7,17,18	2,4,6,9,11,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	3,7,16	2,4,6,9,11	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	3,7,17	2,4,6,9,11,15,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	3,7,16,18	2,4,6,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	3,7,14	2,4,6,9,11	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	3,7,14,16,17,18	2,4,6,9,11,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	3,7,14,18	2,4,6,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	3,7,14,16,17	2,4,6,9,11,15,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	3,7,17	2,4,6,9,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	3,7,16,18	2,4,6,9,11,13,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	3,7,17,18	2,4,6,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	3,7,16	2,4,6,9,11,13,15	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	3,7,14,18	2,4,6,9,11,13,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,7,14,16,17	2,4,6,9,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	3,7,14	2,4,6,9,11,13,15	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	3,7,14,16,17,18	2,4,6,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	3,7,12	2,4,6,9,11	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	3,7,12,16,17,18	2,4,6,9,11,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	3,7,12,18	2,4,6,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	3,7,12,16,17	2,4,6,9,11,15,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	3,7,12,14,17,18	2,4,6,9,11,17,18	2^{-1}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	3,7,12,14,16	2,4,6,9,11	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,7,12,14,17	2,4,6,9,11,15,17	2^{-1}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	3,7,12,14,16,18	2,4,6,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	3,7,12,18	2,4,6,9,11,13,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	3,7,12,16,17	2,4,6,9,11,13,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	3,7,12	2,4,6,9,11,13,15	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	3,7,12,16,17,18	2,4,6,9,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	3,7,12,14,17	2,4,6,9,11,13,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	3,7,12,14,16,18	2,4,6,9,11,13,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	3,7,12,14,17,18	2,4,6,9,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	3,7,12,14,16	2,4,6,9,11,13,15	2^{-23}

Table 0.951 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	3,7,10,18	2,4,6,9,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	3,7,10,16,17	2,4,6,9,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	3,7,10	2,4,6,9,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	3,7,10,16,17,18	2,4,6,9,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	3,7,10,14,17	2,4,6,9,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	3,7,10,14,16,18	2,4,6,9,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	3,7,10,14,17,18	2,4,6,9,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	3,7,10,14,16	2,4,6,9,15	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	3,7,10	2,4,6,9,13	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	3,7,10,16,17,18	2,4,6,9,13,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	3,7,10,18	2,4,6,9,13,15,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	3,7,10,16,17	2,4,6,9,13,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	3,7,10,14,17,18	2,4,6,9,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	3,7,10,14,16	2,4,6,9,13	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,7,10,14,17	2,4,6,9,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	3,7,10,14,16,18	2,4,6,9,13,15,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	3,7,10,12,17	2,4,6,9,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	3,7,10,12,16,18	2,4,6,9,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	3,7,10,12,17,18	2,4,6,9,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	3,7,10,12,16	2,4,6,9,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	3,7,10,12,14,18	2,4,6,9,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	3,7,10,12,14,16,17	2,4,6,9,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	3,7,10,12,14	2,4,6,9,15	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	3,7,10,12,14,16,17,18	2,4,6,9,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	3,7,10,12,17,18	2,4,6,9,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	3,7,10,12,16	2,4,6,9,13	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	3,7,10,12,17	2,4,6,9,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	3,7,10,12,16,18	2,4,6,9,13,15,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	3,7,10,12,14	2,4,6,9,13	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	3,7,10,12,14,16,17,18	2,4,6,9,13,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	3,7,10,12,14,18	2,4,6,9,13,15,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	3,7,10,12,14,16,17	2,4,6,9,13,15,17	$2^{-28.5}$

Table 0.952 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	3,7,10	2,4,6,9,11	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	3,7,10,16,17,18	2,4,6,9,11,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	3,7,10,18	2,4,6,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	3,7,10,16,17	2,4,6,9,11,15,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	3,7,10,14,17,18	2,4,6,9,11,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	3,7,10,14,16	2,4,6,9,11	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,7,10,14,17	2,4,6,9,11,15,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	3,7,10,14,16,18	2,4,6,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	3,7,10,18	2,4,6,9,11,13,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	3,7,10,16,17	2,4,6,9,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	3,7,10	2,4,6,9,11,13,15	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	3,7,10,16,17,18	2,4,6,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	3,7,10,14,17	2,4,6,9,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	3,7,10,14,16,18	2,4,6,9,11,13,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	3,7,10,14,17,18	2,4,6,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	3,7,10,14,16	2,4,6,9,11,13,15	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	3,7,10,12,17,18	2,4,6,9,11,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	3,7,10,12,16	2,4,6,9,11	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	3,7,10,12,17	2,4,6,9,11,15,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	3,7,10,12,16,18	2,4,6,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	3,7,10,12,14	2,4,6,9,11	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,7,10,12,14,16,17,18	2,4,6,9,11,17,18	2^{-34}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	3,7,10,12,14,18	2,4,6,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	3,7,10,12,14,16,17	2,4,6,9,11,15,17	2^{-34}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	3,7,10,12,17	2,4,6,9,11,13,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	3,7,10,12,16,18	2,4,6,9,11,13,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	3,7,10,12,17,18	2,4,6,9,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	3,7,10,12,16	2,4,6,9,11,13,15	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	3,7,10,12,14,18	2,4,6,9,11,13,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,7,10,12,14,16,17	2,4,6,9,11,13,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	3,7,10,12,14	2,4,6,9,11,13,15	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	3,7,10,12,14,16,17,18	2,4,6,9,11,13,15,17,18	$2^{-28.5}$

Table 0.953 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	3,7	2,4,6,8	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	3,7,16,17,18	2,4,6,8,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	3,7,18	2,4,6,8,15,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	3,7,16,17	2,4,6,8,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	3,7,14,17,18	2,4,6,8,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	3,7,14,16	2,4,6,8	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	3,7,14,17	2,4,6,8,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	3,7,14,16,18	2,4,6,8,15,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	3,7,18	2,4,6,8,13,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	3,7,16,17	2,4,6,8,13,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	3,7	2,4,6,8,13,15	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	3,7,16,17,18	2,4,6,8,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	3,7,14,17	2,4,6,8,13,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	3,7,14,16,18	2,4,6,8,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	3,7,14,17,18	2,4,6,8,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,7,14,16	2,4,6,8,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	3,7,12,17,18	2,4,6,8,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	3,7,12,16	2,4,6,8	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	3,7,12,17	2,4,6,8,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	3,7,12,16,18	2,4,6,8,15,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	3,7,12,14	2,4,6,8	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	3,7,12,14,16,17,18	2,4,6,8,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	3,7,12,14,18	2,4,6,8,15,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	3,7,12,14,16,17	2,4,6,8,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	3,7,12,17	2,4,6,8,13,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	3,7,12,16,18	2,4,6,8,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	3,7,12,17,18	2,4,6,8,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	3,7,12,16	2,4,6,8,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	3,7,12,14,18	2,4,6,8,13,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	3,7,12,14,16,17	2,4,6,8,13,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	3,7,12,14	2,4,6,8,13,15	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	3,7,12,14,16,17,18	2,4,6,8,13,15,17,18	2^{-12}

Table 0.954 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	3,7,18	2,4,6,8,11,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	3,7,16,17	2,4,6,8,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	3,7	2,4,6,8,11,15	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	3,7,16,17,18	2,4,6,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	3,7,14,17	2,4,6,8,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	3,7,14,16,18	2,4,6,8,11,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	3,7,14,17,18	2,4,6,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,7,14,16	2,4,6,8,11,15	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	3,7	2,4,6,8,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	3,7,16,17,18	2,4,6,8,11,13,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,7,18	2,4,6,8,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	3,7,16,17	2,4,6,8,11,13,15,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	3,7,14,17,18	2,4,6,8,11,13,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,7,14,16	2,4,6,8,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	3,7,14,17	2,4,6,8,11,13,15,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,7,14,16,18	2,4,6,8,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	3,7,12,17	2,4,6,8,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	3,7,12,16,18	2,4,6,8,11,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	3,7,12,17,18	2,4,6,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	3,7,12,16	2,4,6,8,11,15	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	3,7,12,14,18	2,4,6,8,11,18	2^{-34}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	3,7,12,14,16,17	2,4,6,8,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	3,7,12,14	2,4,6,8,11,15	2^{-34}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	3,7,12,14,16,17,18	2,4,6,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	3,7,12,17,18	2,4,6,8,11,13,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,7,12,16	2,4,6,8,11,13	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	3,7,12,17	2,4,6,8,11,13,15,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,7,12,16,18	2,4,6,8,11,13,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,7,12,14	2,4,6,8,11,13	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	3,7,12,14,16,17,18	2,4,6,8,11,13,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,7,12,14,18	2,4,6,8,11,13,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	3,7,12,14,16,17	2,4,6,8,11,13,15,17	2^{-12}

Table 0.955 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	3,7,10,17,18	2,4,6,8,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	3,7,10,16	2,4,6,8	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	3,7,10,17	2,4,6,8,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	3,7,10,16,18	2,4,6,8,15,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	3,7,10,14	2,4,6,8	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,7,10,14,16,17,18	2,4,6,8,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	3,7,10,14,18	2,4,6,8,15,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	3,7,10,14,16,17	2,4,6,8,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	3,7,10,17	2,4,6,8,13,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	3,7,10,16,18	2,4,6,8,13,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	3,7,10,17,18	2,4,6,8,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	3,7,10,16	2,4,6,8,13,15	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	3,7,10,14,18	2,4,6,8,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	3,7,10,14,16,17	2,4,6,8,13,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	3,7,10,14	2,4,6,8,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	3,7,10,14,16,17,18	2,4,6,8,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	3,7,10,12	2,4,6,8	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	3,7,10,12,16,17,18	2,4,6,8,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	3,7,10,12,18	2,4,6,8,15,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	3,7,10,12,16,17	2,4,6,8,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	3,7,10,12,14,17,18	2,4,6,8,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	3,7,10,12,14,16	2,4,6,8	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	3,7,10,12,14,17	2,4,6,8,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	3,7,10,12,14,16,18	2,4,6,8,15,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	3,7,10,12,18	2,4,6,8,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	3,7,10,12,16,17	2,4,6,8,13,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	3,7,10,12	2,4,6,8,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	3,7,10,12,16,17,18	2,4,6,8,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	3,7,10,12,14,17	2,4,6,8,13,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	3,7,10,12,14,16,18	2,4,6,8,13,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	3,7,10,12,14,17,18	2,4,6,8,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	3,7,10,12,14,16	2,4,6,8,13,15	$2^{-6.5}$

Table 0.956 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	3,7,10,17	2,4,6,8,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	3,7,10,16,18	2,4,6,8,11,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	3,7,10,17,18	2,4,6,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	3,7,10,16	2,4,6,8,11,15	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	3,7,10,14,18	2,4,6,8,11,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	3,7,10,14,16,17	2,4,6,8,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	3,7,10,14	2,4,6,8,11,15	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	3,7,10,14,16,17,18	2,4,6,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	3,7,10,17,18	2,4,6,8,11,13,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	3,7,10,16	2,4,6,8,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	3,7,10,17	2,4,6,8,11,13,15,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	3,7,10,16,18	2,4,6,8,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,7,10,14	2,4,6,8,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	3,7,10,14,16,17,18	2,4,6,8,11,13,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	3,7,10,14,18	2,4,6,8,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	3,7,10,14,16,17	2,4,6,8,11,13,15,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	3,7,10,12,18	2,4,6,8,11,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	3,7,10,12,16,17	2,4,6,8,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	3,7,10,12	2,4,6,8,11,15	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	3,7,10,12,16,17,18	2,4,6,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	3,7,10,12,14,17	2,4,6,8,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	3,7,10,12,14,16,18	2,4,6,8,11,18	2^{-1}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	3,7,10,12,14,17,18	2,4,6,8,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,7,10,12,14,16	2,4,6,8,11,15	2^{-1}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	3,7,10,12	2,4,6,8,11,13	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	3,7,10,12,16,17,18	2,4,6,8,11,13,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	3,7,10,12,18	2,4,6,8,11,13,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	3,7,10,12,16,17	2,4,6,8,11,13,15,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	3,7,10,12,14,17,18	2,4,6,8,11,13,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	3,7,10,12,14,16	2,4,6,8,11,13	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	3,7,10,12,14,17	2,4,6,8,11,13,15,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	3,7,10,12,14,16,18	2,4,6,8,11,13,15,18	$2^{-6.5}$

Table 0.957 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	3,7,18	2,4,6,8,9,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	3,7,16,17	2,4,6,8,9,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	3,7	2,4,6,8,9,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	3,7,16,17,18	2,4,6,8,9,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	3,7,14,17	2,4,6,8,9,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	3,7,14,16,18	2,4,6,8,9,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	3,7,14,17,18	2,4,6,8,9,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	3,7,14,16	2,4,6,8,9,15	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	3,7	2,4,6,8,9,13	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	3,7,16,17,18	2,4,6,8,9,13,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	3,7,18	2,4,6,8,9,13,15,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	3,7,16,17	2,4,6,8,9,13,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	3,7,14,17,18	2,4,6,8,9,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	3,7,14,16	2,4,6,8,9,13	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	3,7,14,17	2,4,6,8,9,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	3,7,14,16,18	2,4,6,8,9,13,15,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	3,7,12,17	2,4,6,8,9,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	3,7,12,16,18	2,4,6,8,9,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	3,7,12,17,18	2,4,6,8,9,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	3,7,12,16	2,4,6,8,9,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	3,7,12,14,18	2,4,6,8,9,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	3,7,12,14,16,17	2,4,6,8,9,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	3,7,12,14	2,4,6,8,9,15	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	3,7,12,14,16,17,18	2,4,6,8,9,15,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	3,7,12,17,18	2,4,6,8,9,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	3,7,12,16	2,4,6,8,9,13	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	3,7,12,17	2,4,6,8,9,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	3,7,12,16,18	2,4,6,8,9,13,15,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	3,7,12,14	2,4,6,8,9,13	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,7,12,14,16,17,18	2,4,6,8,9,13,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	3,7,12,14,18	2,4,6,8,9,13,15,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	3,7,12,14,16,17	2,4,6,8,9,13,15,17	$2^{-6.5}$

Table 0.958 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	3,7	2,4,6,8,9,11	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	3,7,16,17,18	2,4,6,8,9,11,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	3,7,18	2,4,6,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	3,7,16,17	2,4,6,8,9,11,15,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	3,7,14,17,18	2,4,6,8,9,11,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	3,7,14,16	2,4,6,8,9,11	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	3,7,14,17	2,4,6,8,9,11,15,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	3,7,14,16,18	2,4,6,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	3,7,18	2,4,6,8,9,11,13,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	3,7,16,17	2,4,6,8,9,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	3,7	2,4,6,8,9,11,13,15	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	3,7,16,17,18	2,4,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	3,7,14,17	2,4,6,8,9,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	3,7,14,16,18	2,4,6,8,9,11,13,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	3,7,14,17,18	2,4,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	3,7,14,16	2,4,6,8,9,11,13,15	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	3,7,12,17,18	2,4,6,8,9,11,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	3,7,12,16	2,4,6,8,9,11	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	3,7,12,17	2,4,6,8,9,11,15,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	3,7,12,16,18	2,4,6,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	3,7,12,14	2,4,6,8,9,11	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	3,7,12,14,16,17,18	2,4,6,8,9,11,17,18	2^{-1}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	3,7,12,14,18	2,4,6,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	3,7,12,14,16,17	2,4,6,8,9,11,15,17	2^{-1}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	3,7,12,17	2,4,6,8,9,11,13,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	3,7,12,16,18	2,4,6,8,9,11,13,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	3,7,12,17,18	2,4,6,8,9,11,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	3,7,12,16	2,4,6,8,9,11,13,15	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	3,7,12,14,18	2,4,6,8,9,11,13,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	3,7,12,14,16,17	2,4,6,8,9,11,13,17	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	3,7,12,14	2,4,6,8,9,11,13,15	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	3,7,12,14,16,17,18	2,4,6,8,9,11,13,15,17,18	$2^{-6.5}$

Table 0.959 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	3,7,10,17	2,4,6,8,9,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	3,7,10,16,18	2,4,6,8,9,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	3,7,10,17,18	2,4,6,8,9,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,7,10,16	2,4,6,8,9,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	3,7,10,14,18	2,4,6,8,9,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	3,7,10,14,16,17	2,4,6,8,9,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	3,7,10,14	2,4,6,8,9,15	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	3,7,10,14,16,17,18	2,4,6,8,9,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	3,7,10,17,18	2,4,6,8,9,13,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	3,7,10,16	2,4,6,8,9,13	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	3,7,10,17	2,4,6,8,9,13,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	3,7,10,16,18	2,4,6,8,9,13,15,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	3,7,10,14	2,4,6,8,9,13	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	3,7,10,14,16,17,18	2,4,6,8,9,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	3,7,10,14,18	2,4,6,8,9,13,15,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	3,7,10,14,16,17	2,4,6,8,9,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	3,7,10,12,18	2,4,6,8,9,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	3,7,10,12,16,17	2,4,6,8,9,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	3,7,10,12	2,4,6,8,9,15	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	3,7,10,12,16,17,18	2,4,6,8,9,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	3,7,10,12,14,17	2,4,6,8,9,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,7,10,12,14,16,18	2,4,6,8,9,18	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	3,7,10,12,14,17,18	2,4,6,8,9,15,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,7,10,12,14,16	2,4,6,8,9,15	$2^{-6.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	3,7,10,12	2,4,6,8,9,13	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	3,7,10,12,16,17,18	2,4,6,8,9,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	3,7,10,12,18	2,4,6,8,9,13,15,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	3,7,10,12,16,17	2,4,6,8,9,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	3,7,10,12,14,17,18	2,4,6,8,9,13,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,7,10,12,14,16	2,4,6,8,9,13	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	3,7,10,12,14,17	2,4,6,8,9,13,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	3,7,10,12,14,16,18	2,4,6,8,9,13,15,18	2^{-12}

Table 0.960 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	3,7,10,17,18	2,4,6,8,9,11,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	3,7,10,16	2,4,6,8,9,11	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	3,7,10,17	2,4,6,8,9,11,15,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	3,7,10,16,18	2,4,6,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	3,7,10,14	2,4,6,8,9,11	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	3,7,10,14,16,17,18	2,4,6,8,9,11,17,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	3,7,10,14,18	2,4,6,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	3,7,10,14,16,17	2,4,6,8,9,11,15,17	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	3,7,10,17	2,4,6,8,9,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,7,10,16,18	2,4,6,8,9,11,13,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	3,7,10,17,18	2,4,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	3,7,10,16	2,4,6,8,9,11,13,15	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	3,7,10,14,18	2,4,6,8,9,11,13,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	3,7,10,14,16,17	2,4,6,8,9,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	3,7,10,14	2,4,6,8,9,11,13,15	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	3,7,10,14,16,17,18	2,4,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	3,7,10,12	2,4,6,8,9,11	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	3,7,10,12,16,17,18	2,4,6,8,9,11,17,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,7,10,12,18	2,4,6,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	3,7,10,14,16,17	2,4,6,8,9,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	3,7,10,14	2,4,6,8,9,11,13,15	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	3,7,10,12,16,17	2,4,6,8,9,11,15,17	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	3,7,10,12,14,17,18	2,4,6,8,9,11,17,18	2^{-34}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	3,7,10,12,14,16	2,4,6,8,9,11	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	3,7,10,12,14,17	2,4,6,8,9,11,15,17	2^{-34}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	3,7,10,12,14,16,18	2,4,6,8,9,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	3,7,10,12,18	2,4,6,8,9,11,13,18	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	3,7,10,12,16,17	2,4,6,8,9,11,13,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	3,7,10,12	2,4,6,8,9,11,13,15	2^{-23}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	3,7,10,12,16,17,18	2,4,6,8,9,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	3,7,10,12,14,17	2,4,6,8,9,11,13,17	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	3,7,10,12,14,16,18	2,4,6,8,9,11,13,18	2^{-12}
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	3,7,10,12,14,17,18	2,4,6,8,9,11,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	3,7,10,12,14,16	2,4,6,8,9,11,13,15	2^{-12}

Table 0.961 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	3,5	2,4	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	3,5,16,17,18	2,4,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	3,5,18	2,4,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	3,5,16,17	2,4,15,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	3,5,14,17,18	2,4,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	3,5,14,16	2,4	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	3,5,14,17	2,4,15,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	3,5,14,16,18	2,4,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	3,5,18	2,4,13,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,16,17	2,4,13,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	3,5	2,4,13,15	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5,16,17,18	2,4,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	3,5,14,17	2,4,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	3,5,14,16,18	2,4,13,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	3,5,14,17,18	2,4,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	3,5,14,16	2,4,13,15	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	3,5,12,17,18	2,4,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	3,5,12,16	2,4	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	3,5,12,17	2,4,15,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	3,5,12,16,18	2,4,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,12,14	2,4	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	3,5,12,14,16,17,18	2,4,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,12,14,18	2,4,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	3,5,12,14,16,17	2,4,15,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,5,12,17	2,4,13,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,12,16,18	2,4,13,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	3,5,12,17,18	2,4,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,12,16	2,4,13,15	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	3,5,12,14,18	2,4,13,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	3,5,12,14,16,17	2,4,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	3,5,12,14	2,4,13,15	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	3,5,12,14,16,17,18	2,4,13,15,17,18	$2^{-17.5}$

Table 0.962 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	3,5,18	2,4,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	3,5,16,17	2,4,11,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	3,5	2,4,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,5,16,17,18	2,4,11,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	3,5,14,17	2,4,11,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	3,5,14,16,18	2,4,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	3,5,14,17,18	2,4,11,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	3,5,14,16	2,4,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	3,5	2,4,11,13	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	3,5,16,17,18	2,4,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	3,5,18	2,4,11,13,15,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,5,16,17	2,4,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,5,14,17,18	2,4,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	3,5,14,16	2,4,11,13	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,5,14,17	2,4,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	3,5,14,16,18	2,4,11,13,15,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,5,12,17	2,4,11,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	3,5,12,16,18	2,4,11,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	3,5,12,17,18	2,4,11,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	3,5,12,16	2,4,11,15	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	3,5,12,14,18	2,4,11,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	3,5,12,14,16,17	2,4,11,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	3,5,12,14	2,4,11,15	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	3,5,12,14,16,17,18	2,4,11,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,12,17,18	2,4,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,12,16	2,4,11,13	2^{-34}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,12,17	2,4,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	3,5,12,16,18	2,4,11,13,15,18	2^{-34}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	3,5,12,14	2,4,11,13	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	3,5,12,14,16,17,18	2,4,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	3,5,12,14,18	2,4,11,13,15,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	3,5,12,14,16,17	2,4,11,13,15,17	$2^{-17.5}$

Table 0.963 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	3,5,10,17,18	2,4,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	3,5,10,16	2,4	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	3,5,10,17	2,4,15,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	3,5,10,16,18	2,4,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	3,5,10,14	2,4	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	3,5,10,14,16,17,18	2,4,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	3,5,10,14,18	2,4,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	3,5,10,14,16,17	2,4,15,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	3,5,10,17	2,4,13,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	3,5,10,16,18	2,4,13,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	3,5,10,17,18	2,4,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	3,5,10,16	2,4,13,15	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	3,5,10,14,18	2,4,13,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	3,5,10,14,16,17	2,4,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	3,5,10,14	2,4,13,15	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	3,5,10,14,16,17,18	2,4,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5,10,12	2,4	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	3,5,10,12,16,17,18	2,4,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5,10,12,18	2,4,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	3,5,10,12,16,17	2,4,15,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	3,5,10,12,14,17,18	2,4,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	3,5,10,12,14,16	2,4	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	3,5,10,12,14,17	2,4,15,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	3,5,10,12,14,16,18	2,4,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	3,5,10,12,18	2,4,13,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	3,5,10,12,16,17	2,4,13,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	3,5,10,12	2,4,13,15	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	3,5,10,12,16,17,18	2,4,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,10,12,14,17	2,4,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	3,5,10,12,14,16,18	2,4,13,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,10,12,14,17,18	2,4,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	3,5,10,12,14,16	2,4,13,15	2^{-12}

Table 0.964 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,10,17	2,4,11,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	3,5,10,16,18	2,4,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	3,5,10,17,18	2,4,11,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	3,5,10,16	2,4,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	3,5,10,14,18	2,4,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	3,5,10,14,16,17	2,4,11,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	3,5,10,14	2,4,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	3,5,10,14,16,17,18	2,4,11,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	3,5,10,17,18	2,4,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	3,5,10,16	2,4,11,13	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	3,5,10,17	2,4,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	3,5,10,16,18	2,4,11,13,15,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	3,5,10,14	2,4,11,13	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	3,5,10,14,16,17,18	2,4,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	3,5,10,14,18	2,4,11,13,15,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	3,5,10,14,16,17	2,4,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	3,5,10,12,18	2,4,11,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	3,5,10,12,16,17	2,4,11,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	3,5,10,12	2,4,11,15	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	3,5,10,12,16,17,18	2,4,11,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	3,5,10,12,14,17	2,4,11,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	3,5,10,12,14,16,18	2,4,11,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	3,5,10,12,14,17,18	2,4,11,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	3,5,10,12,14,16	2,4,11,15	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	3,5,10,12	2,4,11,13	2^{-1}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,10,12,16,17,18	2,4,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	3,5,10,12,18	2,4,11,13,15,18	2^{-1}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,10,12,16,17	2,4,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	3,5,10,12,14,17,18	2,4,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	3,5,10,12,14,16	2,4,11,13	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	3,5,10,12,14,17	2,4,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	3,5,10,12,14,16,18	2,4,11,13,15,18	2^{-12}

Table 0.965 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	3,5,18	2,4,9,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	3,5,16,17	2,4,9,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	3,5	2,4,9,15	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	3,5,16,17,18	2,4,9,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	3,5,14,17	2,4,9,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	3,5,14,16,18	2,4,9,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	3,5,14,17,18	2,4,9,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	3,5,14,16	2,4,9,15	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	3,5	2,4,9,13	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	3,5,16,17,18	2,4,9,13,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,5,18	2,4,9,13,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	3,5,16,17	2,4,9,13,15,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	3,5,14,17,18	2,4,9,13,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	3,5,14,16	2,4,9,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	3,5,14,17	2,4,9,13,15,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	3,5,14,16,18	2,4,9,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	3,5,12,17	2,4,9,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	3,5,12,16,18	2,4,9,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	3,5,12,17,18	2,4,9,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	3,5,12,16	2,4,9,15	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	3,5,12,14,18	2,4,9,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	3,5,12,14,16,17	2,4,9,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	3,5,12,14	2,4,9,15	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	3,5,12,14,16,17,18	2,4,9,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	3,5,12,17,18	2,4,9,13,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	3,5,12,16	2,4,9,13	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	3,5,12,17	2,4,9,13,15,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	3,5,12,16,18	2,4,9,13,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	3,5,12,14	2,4,9,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	3,5,12,14,16,17,18	2,4,9,13,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	3,5,12,14,18	2,4,9,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	3,5,12,14,16,17	2,4,9,13,15,17	2^{-12}

Table 0.966 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	3,5	2,4,9,11	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	3,5,16,17,18	2,4,9,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	3,5,18	2,4,9,11,15,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	3,5,16,17	2,4,9,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	3,5,14,17,18	2,4,9,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	3,5,14,16	2,4,9,11	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	3,5,14,17	2,4,9,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	3,5,14,16,18	2,4,9,11,15,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	3,5,18	2,4,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	3,5,16,17	2,4,9,11,13,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	3,5	2,4,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	3,5,16,17,18	2,4,9,11,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	3,5,14,17	2,4,9,11,13,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	3,5,14,16,18	2,4,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	3,5,14,17,18	2,4,9,11,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	3,5,14,16	2,4,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	3,5,12,17,18	2,4,9,11,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	3,5,12,16	2,4,9,11	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	3,5,12,17	2,4,9,11,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	3,5,12,16,18	2,4,9,11,15,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	3,5,12,14	2,4,9,11	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	3,5,12,14,16,17,18	2,4,9,11,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	3,5,12,14,18	2,4,9,11,15,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	3,5,12,14,16,17	2,4,9,11,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	3,5,12,17	2,4,9,11,13,17	2^{-1}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	3,5,12,16,18	2,4,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	3,5,12,17,18	2,4,9,11,13,15,17,18	2^{-1}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	3,5,12,16	2,4,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	3,5,12,14,18	2,4,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	3,5,12,14,16,17	2,4,9,11,13,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	3,5,12,14	2,4,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	3,5,12,14,16,17,18	2,4,9,11,13,15,17,18	2^{-12}

Table 0.967 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	3,5,10,17	2,4,9,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	3,5,10,16,18	2,4,9,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	3,5,10,17,18	2,4,9,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	3,5,10,16	2,4,9,15	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	3,5,10,14,18	2,4,9,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	3,5,10,14,16,17	2,4,9,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	3,5,10,14	2,4,9,15	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	3,5,10,14,16,17,18	2,4,9,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,10,17,18	2,4,9,13,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	3,5,10,16	2,4,9,13	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,10,17	2,4,9,13,15,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	3,5,10,16,18	2,4,9,13,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	3,5,10,14	2,4,9,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	3,5,10,14,16,17,18	2,4,9,13,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	3,5,10,14,18	2,4,9,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	3,5,10,14,16,17	2,4,9,13,15,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	3,5,10,12,18	2,4,9,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	3,5,10,12,16,17	2,4,9,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	3,5,10,12	2,4,9,15	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	3,5,10,12,16,17,18	2,4,9,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,5,10,12,14,17	2,4,9,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	3,5,10,12,14,16,18	2,4,9,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	3,5,10,12,14,17,18	2,4,9,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	3,5,10,12,14,16	2,4,9,15	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	3,5,10,12	2,4,9,13	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	3,5,10,12,16,17,18	2,4,9,13,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	3,5,10,12,18	2,4,9,13,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	3,5,10,12,16,17	2,4,9,13,15,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	3,5,10,12,14,17,18	2,4,9,13,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	3,5,10,12,14,16	2,4,9,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	3,5,10,12,14,17	2,4,9,13,15,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	3,5,10,12,14,16,18	2,4,9,13,15,18	$2^{-17.5}$

Table 0.968 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	3,5,10,17,18	2,4,9,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	3,5,10,16	2,4,9,11	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	3,5,10,17	2,4,9,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	3,5,10,16,18	2,4,9,11,15,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	3,5,10,14	2,4,9,11	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,5,10,14,16,17,18	2,4,9,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	3,5,10,14,18	2,4,9,11,15,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	3,5,10,14,16,17	2,4,9,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	3,5,10,17	2,4,9,11,13,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	3,5,10,16,18	2,4,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	3,5,10,17,18	2,4,9,11,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	3,5,10,16	2,4,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	3,5,10,14,18	2,4,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	3,5,10,14,16,17	2,4,9,11,13,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	3,5,10,14	2,4,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	3,5,10,14,16,17,18	2,4,9,11,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,10,12	2,4,9,11	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	3,5,10,12,16,17,18	2,4,9,11,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	3,5,10,12,18	2,4,9,11,15,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	3,5,10,12,16,17	2,4,9,11,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	3,5,10,12,14,17,18	2,4,9,11,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	3,5,10,12,14,16	2,4,9,11	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	3,5,10,12,14,17	2,4,9,11,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	3,5,10,12,14,16,18	2,4,9,11,15,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	3,5,10,12,18	2,4,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	3,5,10,12,16,17	2,4,9,11,13,17	2^{-34}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	3,5,10,12	2,4,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	3,5,10,12,16,17,18	2,4,9,11,13,15,17,18	2^{-34}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,10,12,14,17	2,4,9,11,13,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	3,5,10,12,14,16,18	2,4,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,10,12,14,17,18	2,4,9,11,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	3,5,10,12,14,16	2,4,9,11,13,15	$2^{-17.5}$

Table 0.969 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	3,5,17,18	2,4,8,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	3,5,16	2,4,8	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	3,5,17	2,4,8,15,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,5,16,18	2,4,8,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	3,5,14	2,4,8	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	3,5,14,16,17,18	2,4,8,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	3,5,14,18	2,4,8,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	3,5,14,16,17	2,4,8,15,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	3,5,17	2,4,8,13,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,16,18	2,4,8,13,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	3,5,17,18	2,4,8,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,16	2,4,8,13,15	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	3,5,14,18	2,4,8,13,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	3,5,14,16,17	2,4,8,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	3,5,14	2,4,8,13,15	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	3,5,14,16,17,18	2,4,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	3,5,12	2,4,8	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	3,5,12,16,17,18	2,4,8,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	3,5,12,18	2,4,8,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	3,5,12,16,17	2,4,8,15,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	3,5,12,14,17,18	2,4,8,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,5,12,14,16	2,4,8	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	3,5,12,14,17	2,4,8,15,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	3,5,12,14,16,18	2,4,8,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	3,5,12,18	2,4,8,13,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	3,5,12,16,17	2,4,8,13,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	3,5,12	2,4,8,13,15	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	3,5,12,16,17,18	2,4,8,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	3,5,12,14,17	2,4,8,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	3,5,12,14,16,18	2,4,8,13,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	3,5,12,14,17,18	2,4,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	3,5,12,14,16	2,4,8,13,15	2^{-23}

Table 0.970 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	3,5,17	2,4,8,11,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	3,5,16,18	2,4,8,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	3,5,17,18	2,4,8,11,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	3,5,16	2,4,8,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,5,14,18	2,4,8,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	3,5,14,16,17	2,4,8,11,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	3,5,14	2,4,8,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	3,5,14,16,17,18	2,4,8,11,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	3,5,17,18	2,4,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	3,5,16	2,4,8,11,13	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	3,5,17	2,4,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	3,5,16,18	2,4,8,11,13,15,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	3,5,14	2,4,8,11,13	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	3,5,14,16,17,18	2,4,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	3,5,14,18	2,4,8,11,13,15,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	3,5,14,16,17	2,4,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	3,5,12,18	2,4,8,11,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	3,5,12,16,17	2,4,8,11,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	3,5,12	2,4,8,11,15	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	3,5,12,16,17,18	2,4,8,11,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,5,12,14,17	2,4,8,11,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	3,5,12,14,16,18	2,4,8,11,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	3,5,12,14,17,18	2,4,8,11,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	3,5,12,14,16	2,4,8,11,15	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	3,5,12	2,4,8,11,13	2^{-34}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	3,5,12,16,17,18	2,4,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	3,5,12,18	2,4,8,11,13,15,18	2^{-34}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	3,5,12,16,17	2,4,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	3,5,12,14,17,18	2,4,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,12,14,16	2,4,8,11,13	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	3,5,12,14,17	2,4,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,12,14,16,18	2,4,8,11,13,15,18	2^{-23}

Table 0.971 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	3,5,10	2,4,8	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	3,5,10,16,17,18	2,4,8,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	3,5,10,18	2,4,8,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	3,5,10,16,17	2,4,8,15,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	3,5,10,14,17,18	2,4,8,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	3,5,10,14,16	2,4,8	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	3,5,10,14,17	2,4,8,15,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	3,5,10,14,16,18	2,4,8,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	3,5,10,18	2,4,8,13,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	3,5,10,16,17	2,4,8,13,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	3,5,10	2,4,8,13,15	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,5,10,16,17,18	2,4,8,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	3,5,10,14,17	2,4,8,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	3,5,10,14,16,18	2,4,8,13,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	3,5,10,14,17,18	2,4,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	3,5,10,14,16	2,4,8,13,15	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	3,5,10,12,17,18	2,4,8,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	3,5,10,12,16	2,4,8	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	3,5,10,12,17	2,4,8,15,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	3,5,10,12,16,18	2,4,8,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	3,5,10,12,14	2,4,8	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	3,5,10,12,14,16,17,18	2,4,8,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	3,5,10,12,14,18	2,4,8,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	3,5,10,12,14,16,17	2,4,8,15,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	3,5,10,12,17	2,4,8,13,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	3,5,10,12,16,18	2,4,8,13,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	3,5,10,12,17,18	2,4,8,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	3,5,10,12,16	2,4,8,13,15	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	3,5,10,12,14,18	2,4,8,13,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	3,5,10,12,14,16,17	2,4,8,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	3,5,10,12,14	2,4,8,13,15	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	3,5,10,12,14,16,17,18	2,4,8,13,15,17,18	$2^{-17.5}$

Table 0.972 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	3,5,10,18	2,4,8,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	3,5,10,16,17	2,4,8,11,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	3,5,10	2,4,8,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	3,5,10,16,17,18	2,4,8,11,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	3,5,10,14,17	2,4,8,11,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	3,5,10,14,16,18	2,4,8,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	3,5,10,14,17,18	2,4,8,11,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	3,5,10,14,16	2,4,8,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	3,5,10	2,4,8,11,13	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	3,5,10,16,17,18	2,4,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	3,5,10,18	2,4,8,11,13,15,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	3,5,10,16,17	2,4,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	3,5,10,14,17,18	2,4,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	3,5,10,14,16	2,4,8,11,13	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	3,5,10,14,17	2,4,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	3,5,10,14,16,18	2,4,8,11,13,15,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	3,5,10,12,17	2,4,8,11,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	3,5,10,12,16,18	2,4,8,11,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	3,5,10,12,17,18	2,4,8,11,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	3,5,10,12,16	2,4,8,11,15	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	3,5,10,12,14,18	2,4,8,11,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	3,5,10,12,14,16,17	2,4,8,11,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	3,5,10,12,14	2,4,8,11,15	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	3,5,10,12,14,16,17,18	2,4,8,11,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	3,5,10,12,17,18	2,4,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	3,5,10,12,16	2,4,8,11,13	2^{-1}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	3,5,10,12,17	2,4,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	3,5,10,12,16,18	2,4,8,11,13,15,18	2^{-1}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	3,5,10,12,14	2,4,8,11,13	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	3,5,10,12,14,16,17,18	2,4,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	3,5,10,12,14,18	2,4,8,11,13,15,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	3,5,10,12,14,16,17	2,4,8,11,13,15,17	$2^{-17.5}$

Table 0.973 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	3,5,17	2,4,8,9,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	3,5,16,18	2,4,8,9,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	3,5,17,18	2,4,8,9,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	3,5,16	2,4,8,9,15	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	3,5,14,18	2,4,8,9,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	3,5,14,16,17	2,4,8,9,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	3,5,14	2,4,8,9,15	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	3,5,14,16,17,18	2,4,8,9,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	3,5,17,18	2,4,8,9,13,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	3,5,16	2,4,8,9,13	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	3,5,17	2,4,8,9,13,15,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	3,5,16,18	2,4,8,9,13,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	3,5,14	2,4,8,9,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	3,5,14,16,17,18	2,4,8,9,13,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	3,5,14,18	2,4,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	3,5,14,16,17	2,4,8,9,13,15,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	3,5,12,18	2,4,8,9,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5,12,16,17	2,4,8,9,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	3,5,12	2,4,8,9,15	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5,12,16,17,18	2,4,8,9,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	3,5,12,14,17	2,4,8,9,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	3,5,12,14,16,18	2,4,8,9,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	3,5,12,14,17,18	2,4,8,9,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	3,5,12,14,16	2,4,8,9,15	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	3,5,12	2,4,8,9,13	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	3,5,12,16,17,18	2,4,8,9,13,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	3,5,12,18	2,4,8,9,13,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	3,5,12,16,17	2,4,8,9,13,15,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	3,5,12,14,17,18	2,4,8,9,13,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,12,14,16	2,4,8,9,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	3,5,12,14,17	2,4,8,9,13,15,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,12,14,16,18	2,4,8,9,13,15,18	$2^{-17.5}$

Table 0.974 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	3,5,17,18	2,4,8,9,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,16	2,4,8,9,11	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	3,5,17	2,4,8,9,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	3,5,16,18	2,4,8,9,11,15,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	3,5,14	2,4,8,9,11	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	3,5,14,16,17,18	2,4,8,9,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	3,5,14,18	2,4,8,9,11,15,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	3,5,14,16,17	2,4,8,9,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	3,5,17	2,4,8,9,11,13,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	3,5,16,18	2,4,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	3,5,17,18	2,4,8,9,11,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	3,5,16	2,4,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	3,5,14,18	2,4,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	3,5,14,16,17	2,4,8,9,11,13,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	3,5,14	2,4,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	3,5,14,16,17,18	2,4,8,9,11,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	3,5,12	2,4,8,9,11	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	3,5,12,16,17,18	2,4,8,9,11,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	3,5,12,18	2,4,8,9,11,15,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	3,5,12,16,17	2,4,8,9,11,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	3,5,12,14,17,18	2,4,8,9,11,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	3,5,12,14,16	2,4,8,9,11	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	3,5,12,14,17	2,4,8,9,11,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	3,5,12,14,16,18	2,4,8,9,11,15,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,12,18	2,4,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	3,5,12,16,17	2,4,8,9,11,13,17	2^{-1}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,12	2,4,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	3,5,12,16,17,18	2,4,8,9,11,13,15,17,18	2^{-1}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	3,5,12,14,17	2,4,8,9,11,13,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	3,5,12,14,16,18	2,4,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	3,5,12,14,17,18	2,4,8,9,11,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	3,5,12,14,16	2,4,8,9,11,13,15	$2^{-17.5}$

Table 0.975 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	3,5,10,18	2,4,8,9,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	3,5,10,16,17	2,4,8,9,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	3,5,10	2,4,8,9,15	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	3,5,10,16,17,18	2,4,8,9,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	3,5,10,14,17	2,4,8,9,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	3,5,10,14,16,18	2,4,8,9,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	3,5,10,14,17,18	2,4,8,9,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	3,5,10,14,16	2,4,8,9,15	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	3,5,10	2,4,8,9,13	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	3,5,10,16,17,18	2,4,8,9,13,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	3,5,10,18	2,4,8,9,13,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	3,5,10,16,17	2,4,8,9,13,15,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	3,5,10,14,17,18	2,4,8,9,13,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	3,5,10,14,16	2,4,8,9,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	3,5,10,14,17	2,4,8,9,13,15,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	3,5,10,14,16,18	2,4,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	3,5,10,12,17	2,4,8,9,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	3,5,10,12,16,18	2,4,8,9,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	3,5,10,12,17,18	2,4,8,9,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	3,5,10,12,16	2,4,8,9,15	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	3,5,10,12,14,18	2,4,8,9,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,10,12,14,16,17	2,4,8,9,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	3,5,10,12,14	2,4,8,9,15	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,10,12,14,16,17,18	2,4,8,9,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,10,12,17,18	2,4,8,9,13,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	3,5,10,12,16	2,4,8,9,13	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,10,12,17	2,4,8,9,13,15,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	3,5,10,12,16,18	2,4,8,9,13,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	3,5,10,12,14	2,4,8,9,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	3,5,10,12,14,16,17,18	2,4,8,9,13,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	3,5,10,12,14,18	2,4,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	3,5,10,12,14,16,17	2,4,8,9,13,15,17	2^{-23}

Table 0.976 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	3,5,10	2,4,8,9,11	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	3,5,10,16,17,18	2,4,8,9,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,5,10,18	2,4,8,9,11,15,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	3,5,10,16,17	2,4,8,9,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	3,5,10,14,17,18	2,4,8,9,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	3,5,10,14,16	2,4,8,9,11	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	3,5,10,14,17	2,4,8,9,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	3,5,10,14,16,18	2,4,8,9,11,15,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	3,5,10,18	2,4,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	3,5,10,16,17	2,4,8,9,11,13,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,5,10	2,4,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	3,5,10,16,17,18	2,4,8,9,11,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	3,5,10,14,17	2,4,8,9,11,13,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	3,5,10,14,16,18	2,4,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	3,5,10,14,17,18	2,4,8,9,11,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,5,10,14,16	2,4,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	3,5,10,12,17,18	2,4,8,9,11,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,5,10,12,16	2,4,8,9,11	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	3,5,10,12,17	2,4,8,9,11,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	3,5,10,12,16,18	2,4,8,9,11,15,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	3,5,10,12,14	2,4,8,9,11	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	3,5,10,12,14,16,17,18	2,4,8,9,11,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	3,5,10,12,14,18	2,4,8,9,11,15,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	3,5,10,12,14,16,17	2,4,8,9,11,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	3,5,10,12,17	2,4,8,9,11,13,17	2^{-34}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	3,5,10,12,16,18	2,4,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	3,5,10,12,17,18	2,4,8,9,11,13,15,17,18	2^{-34}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	3,5,10,12,16	2,4,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	3,5,10,12,14,18	2,4,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	3,5,10,12,14,16,17	2,4,8,9,11,13,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	3,5,10,12,14	2,4,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	3,5,10,12,14,16,17,18	2,4,8,9,11,13,15,17,18	2^{-23}

Table 0.977 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	3,5,7,18	2,4,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	3,5,7,16,17	2,4,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	3,5,7	2,4,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	3,5,7,16,17,18	2,4,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	3,5,7,14,17	2,4,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	3,5,7,14,16,18	2,4,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	3,5,7,14,17,18	2,4,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	3,5,7,14,16	2,4,15	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	3,5,7	2,4,13	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	3,5,7,16,17,18	2,4,13,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	3,5,7,18	2,4,13,15,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	3,5,7,16,17	2,4,13,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	3,5,7,14,17,18	2,4,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	3,5,7,14,16	2,4,13	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	3,5,7,14,17	2,4,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	3,5,7,14,16,18	2,4,13,15,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	3,5,7,12,17	2,4,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	3,5,7,12,16,18	2,4,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	3,5,7,12,17,18	2,4,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	3,5,7,12,16	2,4,15	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	3,5,7,12,14,18	2,4,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	3,5,7,12,14,16,17	2,4,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	3,5,7,12,14	2,4,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	3,5,7,12,14,16,17,18	2,4,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	3,5,7,12,17,18	2,4,13,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	3,5,7,12,16	2,4,13	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	3,5,7,12,17	2,4,13,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	3,5,7,12,16,18	2,4,13,15,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	3,5,7,12,14	2,4,13	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	3,5,7,12,14,16,17,18	2,4,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	3,5,7,12,14,18	2,4,13,15,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	3,5,7,12,14,16,17	2,4,13,15,17	$2^{-17.5}$

Table 0.978 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	3,5,7	2,4,11	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	3,5,7,16,17,18	2,4,11,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	3,5,7,18	2,4,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	3,5,7,16,17	2,4,11,15,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	3,5,7,14,17,18	2,4,11,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	3,5,7,14,16	2,4,11	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	3,5,7,14,17	2,4,11,15,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	3,5,7,14,16,18	2,4,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,5,7,18	2,4,11,13,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	3,5,7,16,17	2,4,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	3,5,7	2,4,11,13,15	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	3,5,7,16,17,18	2,4,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	3,5,7,14,17	2,4,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	3,5,7,14,16,18	2,4,11,13,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	3,5,7,14,17,18	2,4,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	3,5,7,14,16	2,4,11,13,15	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	3,5,7,12,17,18	2,4,11,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	3,5,7,12,16	2,4,11	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	3,5,7,12,17	2,4,11,15,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	3,5,7,12,16,18	2,4,11,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	3,5,7,12,14	2,4,11	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	3,5,7,12,14,16,17,18	2,4,11,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	3,5,7,12,14,18	2,4,11,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	3,5,7,12,14,16,17	2,4,11,15,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	3,5,7,12,17	2,4,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	3,5,7,12,16,18	2,4,11,13,18	2^{-34}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	3,5,7,12,17,18	2,4,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	3,5,7,12,16	2,4,11,13,15	2^{-34}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	3,5,7,12,14,18	2,4,11,13,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	3,5,7,12,14,16,17	2,4,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	3,5,7,12,14	2,4,11,13,15	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	3,5,7,12,14,16,17,18	2,4,11,13,15,17,18	$2^{-17.5}$

Table 0.979 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	3,5,7,10,17	2,4,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	3,5,7,10,16,18	2,4,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	3,5,7,10,17,18	2,4,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	3,5,7,10,16	2,4,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	3,5,7,10,14,18	2,4,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	3,5,7,10,14,16,17	2,4,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,5,7,10,14	2,4,15	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,5,7,10,14,16,17,18	2,4,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	3,5,7,10,17,18	2,4,13,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	3,5,7,10,16	2,4,13	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	3,5,7,10,17	2,4,13,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	3,5,7,10,16,18	2,4,13,15,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	3,5,7,10,14	2,4,13	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	3,5,7,10,14,16,17,18	2,4,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	3,5,7,10,14,18	2,4,13,15,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	3,5,7,10,14,16,17	2,4,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	3,5,7,10,12,18	2,4,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	3,5,7,10,12,16,17	2,4,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	3,5,7,10,12	2,4,15	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	3,5,7,10,12,16,17,18	2,4,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	3,5,7,10,12,14,17	2,4,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	3,5,7,10,12,14,16,18	2,4,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	3,5,7,10,12,14,17,18	2,4,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	3,5,7,10,12,14,16	2,4,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	3,5,7,10,12	2,4,13	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	3,5,7,10,12,16,17,18	2,4,13,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	3,5,7,10,12,18	2,4,13,15,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	3,5,7,10,12,16,17	2,4,13,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,7,10,12,14,17,18	2,4,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	3,5,7,10,12,14,16	2,4,13	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,7,10,12,14,17	2,4,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	3,5,7,10,12,14,16,18	2,4,13,15,18	2^{-12}

Table 0.980 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,5,7,10,17,18	2,4,11,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	3,5,7,10,16	2,4,11	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	3,5,7,10,17	2,4,11,15,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	3,5,7,10,16,18	2,4,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	3,5,7,10,14	2,4,11	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	3,5,7,10,14,16,17,18	2,4,11,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	3,5,7,10,14,18	2,4,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	3,5,7,10,14,16,17	2,4,11,15,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,7,10,17	2,4,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	3,5,7,10,16,18	2,4,11,13,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,7,10,17,18	2,4,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	3,5,7,10,16	2,4,11,13,15	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	3,5,7,10,14,18	2,4,11,13,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	3,5,7,10,14,16,17	2,4,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	3,5,7,10,14	2,4,11,13,15	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	3,5,7,10,14,16,17,18	2,4,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	3,5,7,10,12	2,4,11	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	3,5,7,10,12,16,17,18	2,4,11,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	3,5,7,10,12,18	2,4,11,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	3,5,7,10,12,16,17	2,4,11,15,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	3,5,7,10,12,14,17,18	2,4,11,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	3,5,7,10,12,14,16	2,4,11	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,5,7,10,12,14,17	2,4,11,15,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	3,5,7,10,12,14,16,18	2,4,11,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	3,5,7,10,12,18	2,4,11,13,18	2^{-1}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	3,5,7,10,12,16,17	2,4,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	3,5,7,10,12	2,4,11,13,15	2^{-1}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	3,5,7,10,12,16,17,18	2,4,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	3,5,7,10,12,14,17	2,4,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	3,5,7,10,12,14,16,18	2,4,11,13,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	3,5,7,10,12,14,17,18	2,4,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	3,5,7,10,12,14,16	2,4,11,13,15	2^{-12}

Table 0.981 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	3,5,7	2,4,9	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,5,7,16,17,18	2,4,9,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	3,5,7,18	2,4,9,15,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	3,5,7,16,17	2,4,9,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,14,17,18	2,4,9,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	3,5,7,14,16	2,4,9	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,14,17	2,4,9,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	3,5,7,14,16,18	2,4,9,15,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	3,5,7,18	2,4,9,13,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,5,7,16,17	2,4,9,13,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	3,5,7	2,4,9,13,15	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,5,7,16,17,18	2,4,9,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,5,7,14,17	2,4,9,13,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	3,5,7,14,16,18	2,4,9,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,5,7,14,17,18	2,4,9,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	3,5,7,14,16	2,4,9,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,12,17,18	2,4,9,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,12,16	2,4,9	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,5,7,12,17	2,4,9,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	3,5,7,12,16,18	2,4,9,15,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,12,14	2,4,9	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	3,5,7,12,14,16,17,18	2,4,9,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,12,14,18	2,4,9,15,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	3,5,7,12,14,16,17	2,4,9,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,12,17	2,4,9,13,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,12,16,18	2,4,9,13,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,12,17,18	2,4,9,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,12,16	2,4,9,13,15	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,12,14,18	2,4,9,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,5,7,12,14,16,17	2,4,9,13,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,12,14	2,4,9,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	3,5,7,12,14,16,17,18	2,4,9,13,15,17,18	2^{-12}

Table 0.982 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	3,5,7,18	2,4,9,11,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	3,5,7,16,17	2,4,9,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	3,5,7	2,4,9,11,15	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	3,5,7,16,17,18	2,4,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	3,5,7,14,17	2,4,9,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	3,5,7,14,16,18	2,4,9,11,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	3,5,7,14,17,18	2,4,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	3,5,7,14,16	2,4,9,11,15	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	3,5,7	2,4,9,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	3,5,7,16,17,18	2,4,9,11,13,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	3,5,7,18	2,4,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	3,5,7,16,17	2,4,9,11,13,15,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	3,5,7,14,17,18	2,4,9,11,13,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	3,5,7,14,16	2,4,9,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	3,5,7,14,17	2,4,9,11,13,15,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	3,5,7,14,16,18	2,4,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	3,5,7,12,17	2,4,9,11,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	3,5,7,12,16,18	2,4,9,11,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	3,5,7,12,17,18	2,4,9,11,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	3,5,7,12,16	2,4,9,11,15	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,7,12,14,18	2,4,9,11,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	3,5,7,12,14,16,17	2,4,9,11,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,7,12,14	2,4,9,11,15	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	3,5,7,12,14,16,17,18	2,4,9,11,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	3,5,7,12,17,18	2,4,9,11,13,17,18	2^{-1}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,7,12,16	2,4,9,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	3,5,7,12,17	2,4,9,11,13,15,17	2^{-1}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,7,12,16,18	2,4,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	3,5,7,12,14	2,4,9,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	3,5,7,12,14,16,17,18	2,4,9,11,13,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	3,5,7,12,14,18	2,4,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	3,5,7,12,14,16,17	2,4,9,11,13,15,17	2^{-12}

Table 0.983 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	3,5,7,10,17,18	2,4,9,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	3,5,7,10,16	2,4,9	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,7,10,17	2,4,9,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	3,5,7,10,16,18	2,4,9,15,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	3,5,7,10,14	2,4,9	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	3,5,7,10,14,16,17,18	2,4,9,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	3,5,7,10,14,18	2,4,9,15,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	3,5,7,10,14,16,17	2,4,9,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	3,5,7,10,17	2,4,9,13,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	3,5,7,10,16,18	2,4,9,13,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	3,5,7,10,17,18	2,4,9,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	3,5,7,10,16	2,4,9,13,15	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	3,5,7,10,14,18	2,4,9,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	3,5,7,10,14,16,17	2,4,9,13,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	3,5,7,10,14	2,4,9,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	3,5,7,10,14,16,17,18	2,4,9,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,10,12	2,4,9	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	3,5,7,10,12,16,17,18	2,4,9,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,10,12,18	2,4,9,15,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	3,5,7,10,12,16,17	2,4,9,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	3,5,7,10,12,14,17,18	2,4,9,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,10,12,14,16	2,4,9	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	3,5,7,10,12,14,17	2,4,9,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,10,12,14,16,18	2,4,9,15,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	3,5,7,10,12,18	2,4,9,13,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,7,10,12,16,17	2,4,9,13,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	3,5,7,10,12	2,4,9,13,15	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,7,10,12,16,17,18	2,4,9,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	3,5,7,10,12,14,17	2,4,9,13,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	3,5,7,10,12,14,16,18	2,4,9,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,10,12,14,17,18	2,4,9,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	3,5,7,10,12,14,16	2,4,9,13,15	$2^{-17.5}$

Table 0.984 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	3,5,7,10,17	2,4,9,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	3,5,7,10,16,18	2,4,9,11,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	3,5,7,10,17,18	2,4,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	3,5,7,10,16	2,4,9,11,15	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	3,5,7,10,14,18	2,4,9,11,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	3,5,7,10,14,16,17	2,4,9,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	3,5,7,10,14	2,4,9,11,15	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	3,5,7,10,14,16,17,18	2,4,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	3,5,7,10,17,18	2,4,9,11,13,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	3,5,7,10,16	2,4,9,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	3,5,7,10,17	2,4,9,11,13,15,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	3,5,7,10,16,18	2,4,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	3,5,7,10,14	2,4,9,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	3,5,7,10,14,16,17,18	2,4,9,11,13,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	3,5,7,10,14,18	2,4,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	3,5,7,10,14,16,17	2,4,9,11,13,15,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5,7,10,12,18	2,4,9,11,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	3,5,7,10,12,16,17	2,4,9,11,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5,7,10,12	2,4,9,11,15	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	3,5,7,10,12,16,17,18	2,4,9,11,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	3,5,7,10,12,14,17	2,4,9,11,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	3,5,7,10,12,14,16,18	2,4,9,11,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	3,5,7,10,12,14,17,18	2,4,9,11,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	3,5,7,10,12,14,16	2,4,9,11,15	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	3,5,7,10,12	2,4,9,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	3,5,7,10,12,16,17,18	2,4,9,11,13,17,18	2^{-34}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	3,5,7,10,12,18	2,4,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	3,5,7,10,12,16,17	2,4,9,11,13,15,17	2^{-34}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,7,10,12,14,17,18	2,4,9,11,13,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	3,5,7,10,12,14,16	2,4,9,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,7,10,12,14,17	2,4,9,11,13,15,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	3,5,7,10,12,14,16,18	2,4,9,11,13,15,18	$2^{-17.5}$

Table 0.985 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	3,5,7,17	2,4,8,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	3,5,7,16,18	2,4,8,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	3,5,7,17,18	2,4,8,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,7,16	2,4,8,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	3,5,7,14,18	2,4,8,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	3,5,7,14,16,17	2,4,8,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	3,5,7,14	2,4,8,15	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	3,5,7,14,16,17,18	2,4,8,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	3,5,7,17,18	2,4,8,13,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	3,5,7,16	2,4,8,13	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	3,5,7,17	2,4,8,13,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	3,5,7,16,18	2,4,8,13,15,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	3,5,7,14	2,4,8,13	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	3,5,7,14,16,17,18	2,4,8,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	3,5,7,14,18	2,4,8,13,15,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	3,5,7,14,16,17	2,4,8,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	3,5,7,12,18	2,4,8,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,12,16,17	2,4,8,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	3,5,7,12	2,4,8,15	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,12,16,17,18	2,4,8,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,12,14,17	2,4,8,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	3,5,7,12,14,16,18	2,4,8,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,12,14,17,18	2,4,8,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	3,5,7,12,14,16	2,4,8,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,7,12	2,4,8,13	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5,7,12,16,17,18	2,4,8,13,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,7,12,18	2,4,8,13,15,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	3,5,7,12,16,17	2,4,8,13,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	3,5,7,12,14,17,18	2,4,8,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	3,5,7,12,14,16	2,4,8,13	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	3,5,7,12,14,17	2,4,8,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	3,5,7,12,14,16,18	2,4,8,13,15,18	2^{-23}

Table 0.986 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	3,5,7,17,18	2,4,8,11,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	3,5,7,16	2,4,8,11	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	3,5,7,17	2,4,8,11,15,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	3,5,7,16,18	2,4,8,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	3,5,7,14	2,4,8,11	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	3,5,7,14,16,17,18	2,4,8,11,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	3,5,7,14,18	2,4,8,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	3,5,7,14,16,17	2,4,8,11,15,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	3,5,7,17	2,4,8,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	3,5,7,16,18	2,4,8,11,13,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	3,5,7,17,18	2,4,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	3,5,7,16	2,4,8,11,13,15	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	3,5,7,14,18	2,4,8,11,13,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	3,5,7,14,16,17	2,4,8,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	3,5,7,14	2,4,8,11,13,15	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	3,5,7,14,16,17,18	2,4,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	3,5,7,12	2,4,8,11	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5,7,12,16,17,18	2,4,8,11,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	3,5,7,12,18	2,4,8,11,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5,7,12,16,17	2,4,8,11,15,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	3,5,7,12,14,17,18	2,4,8,11,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	3,5,7,12,14,16	2,4,8,11	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	3,5,7,12,14,17	2,4,8,11,15,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	3,5,7,12,14,16,18	2,4,8,11,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	3,5,7,12,18	2,4,8,11,13,18	2^{-34}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	3,5,7,12,16,17	2,4,8,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	3,5,7,12	2,4,8,11,13,15	2^{-34}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	3,5,7,12,16,17,18	2,4,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	3,5,7,12,14,17	2,4,8,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,7,12,14,16,18	2,4,8,11,13,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	3,5,7,12,14,17,18	2,4,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,7,12,14,16	2,4,8,11,13,15	2^{-23}

Table 0.987 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,5,7,10,18	2,4,8,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	3,5,7,10,16,17	2,4,8,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	3,5,7,10	2,4,8,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	3,5,7,10,16,17,18	2,4,8,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	3,5,7,10,14,17	2,4,8,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	3,5,7,10,14,16,18	2,4,8,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	3,5,7,10,14,17,18	2,4,8,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	3,5,7,10,14,16	2,4,8,15	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,5,7,10	2,4,8,13	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	3,5,7,10,16,17,18	2,4,8,13,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,5,7,10,18	2,4,8,13,15,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	3,5,7,10,16,17	2,4,8,13,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	3,5,7,10,14,17,18	2,4,8,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,5,7,10,14,16	2,4,8,13	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	3,5,7,10,14,17	2,4,8,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	3,5,7,10,14,16,18	2,4,8,13,15,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	3,5,7,10,12,17	2,4,8,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,10,12,16,18	2,4,8,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	3,5,7,10,12,17,18	2,4,8,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,10,12,16	2,4,8,15	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5,7,10,12,14,18	2,4,8,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	3,5,7,10,12,14,16,17	2,4,8,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	3,5,7,10,12,14	2,4,8,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	3,5,7,10,12,14,16,17,18	2,4,8,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,10,12,17,18	2,4,8,13,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,10,12,16	2,4,8,13	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,10,12,17	2,4,8,13,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,10,12,16,18	2,4,8,13,15,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,5,7,10,12,14	2,4,8,13	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,10,12,14,16,17,18	2,4,8,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,5,7,10,12,14,18	2,4,8,13,15,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,10,12,14,16,17	2,4,8,13,15,17	$2^{-17.5}$

Table 0.988 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	3,5,7,10	2,4,8,11	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	3,5,7,10,16,17,18	2,4,8,11,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	3,5,7,10,18	2,4,8,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	3,5,7,10,16,17	2,4,8,11,15,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	3,5,7,10,14,17,18	2,4,8,11,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	3,5,7,10,14,16	2,4,8,11	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	3,5,7,10,14,17	2,4,8,11,15,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	3,5,7,10,14,16,18	2,4,8,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	3,5,7,10,18	2,4,8,11,13,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	3,5,7,10,16,17	2,4,8,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	3,5,7,10	2,4,8,11,13,15	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	3,5,7,10,16,17,18	2,4,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	3,5,7,10,14,17	2,4,8,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	3,5,7,10,14,16,18	2,4,8,11,13,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	3,5,7,10,14,17,18	2,4,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,7,10,14,16	2,4,8,11,13,15	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	3,5,7,10,12,17,18	2,4,8,11,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	3,5,7,10,12,16	2,4,8,11	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	3,5,7,10,12,17	2,4,8,11,15,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	3,5,7,10,12,16,18	2,4,8,11,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	3,5,7,10,12,14	2,4,8,11	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,7,10,12,14,16,17,18	2,4,8,11,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	3,5,7,10,12,14,18	2,4,8,11,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,7,10,12,14,16,17	2,4,8,11,15,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,7,10,12,17	2,4,8,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	3,5,7,10,12,16,18	2,4,8,11,13,18	2^{-1}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,7,10,12,17,18	2,4,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	3,5,7,10,12,16	2,4,8,11,13,15	2^{-1}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	3,5,7,10,12,14,18	2,4,8,11,13,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	3,5,7,10,12,14,16,17	2,4,8,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	3,5,7,10,12,14	2,4,8,11,13,15	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	3,5,7,10,12,14,16,17,18	2,4,8,11,13,15,17,18	$2^{-17.5}$

Table 0.989 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	3,5,7,17,18	2,4,8,9,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	3,5,7,16	2,4,8,9	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	3,5,7,17	2,4,8,9,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	3,5,7,16,18	2,4,8,9,15,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	3,5,7,14	2,4,8,9	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	3,5,7,14,16,17,18	2,4,8,9,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,5,7,14,18	2,4,8,9,15,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,5,7,14,16,17	2,4,8,9,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	3,5,7,17	2,4,8,9,13,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	3,5,7,16,18	2,4,8,9,13,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	3,5,7,17,18	2,4,8,9,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	3,5,7,16	2,4,8,9,13,15	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	3,5,7,14,18	2,4,8,9,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	3,5,7,14,16,17	2,4,8,9,13,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	3,5,7,14	2,4,8,9,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	3,5,7,14,16,17,18	2,4,8,9,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	3,5,7,12	2,4,8,9	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,5,7,12,16,17,18	2,4,8,9,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	3,5,7,12,18	2,4,8,9,15,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	3,5,7,12,16,17	2,4,8,9,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	3,5,7,12,14,17,18	2,4,8,9,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	3,5,7,12,14,16	2,4,8,9	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,5,7,12,14,17	2,4,8,9,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	3,5,7,12,14,16,18	2,4,8,9,15,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	3,5,7,12,18	2,4,8,9,13,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	3,5,7,12,16,17	2,4,8,9,13,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	3,5,7,12	2,4,8,9,13,15	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	3,5,7,12,16,17,18	2,4,8,9,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	3,5,7,12,14,17	2,4,8,9,13,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,7,12,14,16,18	2,4,8,9,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	3,5,7,12,14,17,18	2,4,8,9,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,7,12,14,16	2,4,8,9,13,15	$2^{-17.5}$

Table 0.990 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	3,5,7,17	2,4,8,9,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,5,7,16,18	2,4,8,9,11,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	3,5,7,17,18	2,4,8,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	3,5,7,16	2,4,8,9,11,15	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	3,5,7,14,18	2,4,8,9,11,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	3,5,7,14,16,17	2,4,8,9,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	3,5,7,14	2,4,8,9,11,15	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	3,5,7,14,16,17,18	2,4,8,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	3,5,7,17,18	2,4,8,9,11,13,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,7,16	2,4,8,9,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	3,5,7,17	2,4,8,9,11,13,15,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,7,16,18	2,4,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	3,5,7,14	2,4,8,9,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	3,5,7,14,16,17,18	2,4,8,9,11,13,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	3,5,7,14,18	2,4,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	3,5,7,14,16,17	2,4,8,9,11,13,15,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	3,5,7,12,18	2,4,8,9,11,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	3,5,7,12,16,17	2,4,8,9,11,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	3,5,7,12	2,4,8,9,11,15	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	3,5,7,12,16,17,18	2,4,8,9,11,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	3,5,7,12,14,17	2,4,8,9,11,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	3,5,7,12,14,16,18	2,4,8,9,11,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	3,5,7,12,14,17,18	2,4,8,9,11,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,5,7,12,14,16	2,4,8,9,11,15	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	3,5,7,12	2,4,8,9,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	3,5,7,12,16,17,18	2,4,8,9,11,13,17,18	2^{-1}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	3,5,7,12,18	2,4,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	3,5,7,12,16,17	2,4,8,9,11,13,15,17	2^{-1}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	3,5,7,12,14,17,18	2,4,8,9,11,13,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	3,5,7,12,14,16	2,4,8,9,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	3,5,7,12,14,17	2,4,8,9,11,13,15,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	3,5,7,12,14,16,18	2,4,8,9,11,13,15,18	$2^{-17.5}$

Table 0.991 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	3,5,7,10	2,4,8,9	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	3,5,7,10,16,17,18	2,4,8,9,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	3,5,7,10,18	2,4,8,9,15,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	3,5,7,10,16,17	2,4,8,9,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	3,5,7,10,14,17,18	2,4,8,9,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	3,5,7,10,14,16	2,4,8,9	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	3,5,7,10,14,17	2,4,8,9,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	3,5,7,10,14,16,18	2,4,8,9,15,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	3,5,7,10,18	2,4,8,9,13,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	3,5,7,10,16,17	2,4,8,9,13,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	3,5,7,10	2,4,8,9,13,15	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	3,5,7,10,16,17,18	2,4,8,9,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	3,5,7,10,14,17	2,4,8,9,13,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	3,5,7,10,14,16,18	2,4,8,9,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	3,5,7,10,14,17,18	2,4,8,9,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	3,5,7,10,14,16	2,4,8,9,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	3,5,7,10,12,17,18	2,4,8,9,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	3,5,7,10,12,16	2,4,8,9	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	3,5,7,10,12,17	2,4,8,9,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	3,5,7,10,12,16,18	2,4,8,9,15,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	3,5,7,10,12,14	2,4,8,9	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	3,5,7,10,12,14,16,17,18	2,4,8,9,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	3,5,7,10,12,14,18	2,4,8,9,15,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	3,5,7,10,12,14,16,17	2,4,8,9,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	3,5,7,10,12,17	2,4,8,9,13,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	3,5,7,10,12,16,18	2,4,8,9,13,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	3,5,7,10,12,17,18	2,4,8,9,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	3,5,7,10,12,16	2,4,8,9,13,15	$2^{-6.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	3,5,7,10,12,14,18	2,4,8,9,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	3,5,7,10,12,14,16,17	2,4,8,9,13,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	3,5,7,10,12,14	2,4,8,9,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	3,5,7,10,12,14,16,17,18	2,4,8,9,13,15,17,18	2^{-23}

Table 0.992 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	3,5,7,10,18	2,4,8,9,11,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	3,5,7,10,16,17	2,4,8,9,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	3,5,7,10	2,4,8,9,11,15	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	3,5,7,10,16,17,18	2,4,8,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	3,5,7,10,14,17	2,4,8,9,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	3,5,7,10,14,16,18	2,4,8,9,11,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	3,5,7,10,14,17,18	2,4,8,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	3,5,7,10,14,16	2,4,8,9,11,15	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	3,5,7,10	2,4,8,9,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,5,7,10,16,17,18	2,4,8,9,11,13,17,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	3,5,7,10,18	2,4,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	3,5,7,10,16,17	2,4,8,9,11,13,15,17	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	3,5,7,10,14,17,18	2,4,8,9,11,13,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	3,5,7,10,14,16	2,4,8,9,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	3,5,7,10,14,17	2,4,8,9,11,13,15,17	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	3,5,7,10,14,16,18	2,4,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	3,5,7,10,12,17	2,4,8,9,11,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	3,5,7,10,12,16,18	2,4,8,9,11,18	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	3,5,7,10,12,17,18	2,4,8,9,11,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	3,5,7,10,12,16	2,4,8,9,11,15	2^{-12}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	3,5,7,10,12,14,18	2,4,8,9,11,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	3,5,7,10,12,14,16,17	2,4,8,9,11,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	3,5,7,10,12,14	2,4,8,9,11,15	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	3,5,7,10,12,14,16,17,18	2,4,8,9,11,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	3,5,7,10,12,17,18	2,4,8,9,11,13,17,18	2^{-34}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	3,5,7,10,12,16	2,4,8,9,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	3,5,7,10,12,17	2,4,8,9,11,13,15,17	2^{-34}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	3,5,7,10,12,16,18	2,4,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	3,5,7,10,12,14	2,4,8,9,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	3,5,7,10,12,14,16,17,18	2,4,8,9,11,13,17,18	2^{-23}
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	3,5,7,10,12,14,18	2,4,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	3,5,7,10,12,14,16,17	2,4,8,9,11,13,15,17	2^{-23}

Table 0.993 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	3,5,17,18	2,4,6,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	3,5,16	2,4,6	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	3,5,17	2,4,6,15,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	3,5,16,18	2,4,6,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5,14	2,4,6	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	3,5,14,16,17,18	2,4,6,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5,14,18	2,4,6,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	3,5,14,16,17	2,4,6,15,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,17	2,4,6,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	3,5,16,18	2,4,6,13,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,17,18	2,4,6,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	3,5,16	2,4,6,13,15	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	3,5,14,18	2,4,6,13,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	3,5,14,16,17	2,4,6,13,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	3,5,14	2,4,6,13,15	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	3,5,14,16,17,18	2,4,6,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	3,5,12	2,4,6	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	3,5,12,16,17,18	2,4,6,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	3,5,12,18	2,4,6,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	3,5,12,16,17	2,4,6,15,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	3,5,12,14,17,18	2,4,6,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	3,5,12,14,16	2,4,6	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	3,5,12,14,17	2,4,6,15,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	3,5,12,14,16,18	2,4,6,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	3,5,12,18	2,4,6,13,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	3,5,12,16,17	2,4,6,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	3,5,12	2,4,6,13,15	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	3,5,12,16,17,18	2,4,6,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	3,5,12,14,17	2,4,6,13,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	3,5,12,14,16,18	2,4,6,13,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	3,5,12,14,17,18	2,4,6,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	3,5,12,14,16	2,4,6,13,15	2^{-23}

Table 0.994 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	3,5,17	2,4,6,11,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	3,5,16,18	2,4,6,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	3,5,17,18	2,4,6,11,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	3,5,16	2,4,6,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	3,5,14,18	2,4,6,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	3,5,14,16,17	2,4,6,11,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	3,5,14	2,4,6,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	3,5,14,16,17,18	2,4,6,11,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	3,5,17,18	2,4,6,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	3,5,16	2,4,6,11,13	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	3,5,17	2,4,6,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	3,5,16,18	2,4,6,11,13,15,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	3,5,14	2,4,6,11,13	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,14,16,17,18	2,4,6,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	3,5,14,18	2,4,6,11,13,15,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,14,16,17	2,4,6,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	3,5,12,18	2,4,6,11,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	3,5,12,16,17	2,4,6,11,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	3,5,12	2,4,6,11,15	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	3,5,12,16,17,18	2,4,6,11,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,12,14,17	2,4,6,11,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	3,5,12,14,16,18	2,4,6,11,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	3,5,12,14,17,18	2,4,6,11,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	3,5,12,14,16	2,4,6,11,15	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	3,5,12	2,4,6,11,13	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	3,5,12,16,17,18	2,4,6,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	3,5,12,18	2,4,6,11,13,15,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	3,5,12,16,17	2,4,6,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	3,5,12,14,17,18	2,4,6,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	3,5,12,14,16	2,4,6,11,13	2^{-34}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	3,5,12,14,17	2,4,6,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	3,5,12,14,16,18	2,4,6,11,13,15,18	2^{-34}

Table 0.995 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,10	2,4,6	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	3,5,10,16,17,18	2,4,6,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,10,18	2,4,6,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	3,5,10,16,17	2,4,6,15,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	3,5,10,14,17,18	2,4,6,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	3,5,10,14,16	2,4,6	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	3,5,10,14,17	2,4,6,15,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	3,5,10,14,16,18	2,4,6,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	3,5,10,18	2,4,6,13,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	3,5,10,16,17	2,4,6,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	3,5,10	2,4,6,13,15	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	3,5,10,16,17,18	2,4,6,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	3,5,10,14,17	2,4,6,13,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,10,14,16,18	2,4,6,13,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	3,5,10,14,17,18	2,4,6,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,10,14,16	2,4,6,13,15	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	3,5,10,12,17,18	2,4,6,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	3,5,10,12,16	2,4,6	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	3,5,10,12,17	2,4,6,15,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	3,5,10,12,16,18	2,4,6,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	3,5,10,12,14	2,4,6	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	3,5,10,12,14,16,17,18	2,4,6,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	3,5,10,12,14,18	2,4,6,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	3,5,10,12,14,16,17	2,4,6,15,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	3,5,10,12,17	2,4,6,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	3,5,10,12,16,18	2,4,6,13,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	3,5,10,12,17,18	2,4,6,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	3,5,10,12,16	2,4,6,13,15	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	3,5,10,12,14,18	2,4,6,13,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	3,5,10,12,14,16,17	2,4,6,13,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	3,5,10,12,14	2,4,6,13,15	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	3,5,10,12,14,16,17,18	2,4,6,13,15,17,18	$2^{-28.5}$

Table 0.996 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	3,5,10,18	2,4,6,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	3,5,10,16,17	2,4,6,11,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	3,5,10	2,4,6,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	3,5,10,16,17,18	2,4,6,11,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,5,10,14,17	2,4,6,11,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	3,5,10,14,16,18	2,4,6,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	3,5,10,14,17,18	2,4,6,11,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	3,5,10,14,16	2,4,6,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	3,5,10	2,4,6,11,13	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	3,5,10,16,17,18	2,4,6,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	3,5,10,18	2,4,6,11,13,15,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	3,5,10,16,17	2,4,6,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	3,5,10,14,17,18	2,4,6,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	3,5,10,14,16	2,4,6,11,13	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	3,5,10,14,17	2,4,6,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	3,5,10,14,16,18	2,4,6,11,13,15,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	3,5,10,12,17	2,4,6,11,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	3,5,10,12,16,18	2,4,6,11,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	3,5,10,12,17,18	2,4,6,11,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	3,5,10,12,16	2,4,6,11,15	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	3,5,10,12,14,18	2,4,6,11,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	3,5,10,12,14,16,17	2,4,6,11,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	3,5,10,12,14	2,4,6,11,15	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,5,10,12,14,16,17,18	2,4,6,11,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	3,5,10,12,17,18	2,4,6,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	3,5,10,12,16	2,4,6,11,13	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	3,5,10,12,17	2,4,6,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	3,5,10,12,16,18	2,4,6,11,13,15,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	3,5,10,12,14	2,4,6,11,13	2^{-1}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	3,5,10,12,14,16,17,18	2,4,6,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	3,5,10,12,14,18	2,4,6,11,13,15,18	2^{-1}
$(0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,5,10,12,14,16,17	2,4,6,11,13,15,17	$2^{-17.5}$

Table 0.997 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,5,17	2,4,6,9,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	3,5,16,18	2,4,6,9,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	3,5,17,18	2,4,6,9,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	3,5,16	2,4,6,9,15	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	3,5,14,18	2,4,6,9,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	3,5,14,16,17	2,4,6,9,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	3,5,14	2,4,6,9,15	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	3,5,14,16,17,18	2,4,6,9,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	3,5,17,18	2,4,6,9,13,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	3,5,16	2,4,6,9,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	3,5,17	2,4,6,9,13,15,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	3,5,16,18	2,4,6,9,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	3,5,14	2,4,6,9,13	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	3,5,14,16,17,18	2,4,6,9,13,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	3,5,14,18	2,4,6,9,13,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	3,5,14,16,17	2,4,6,9,13,15,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	3,5,12,18	2,4,6,9,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	3,5,12,16,17	2,4,6,9,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	3,5,12	2,4,6,9,15	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	3,5,12,16,17,18	2,4,6,9,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	3,5,12,14,17	2,4,6,9,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	3,5,12,14,16,18	2,4,6,9,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,5,12,14,17,18	2,4,6,9,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	3,5,12,14,16	2,4,6,9,15	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	3,5,12	2,4,6,9,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	3,5,12,16,17,18	2,4,6,9,13,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	3,5,12,18	2,4,6,9,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	3,5,12,16,17	2,4,6,9,13,15,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,12,14,17,18	2,4,6,9,13,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	3,5,12,14,16	2,4,6,9,13	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,12,14,17	2,4,6,9,13,15,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	3,5,12,14,16,18	2,4,6,9,13,15,18	$2^{-28.5}$

Table 0.998 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	3,5,17,18	2,4,6,9,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	3,5,16	2,4,6,9,11	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	3,5,17	2,4,6,9,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	3,5,16,18	2,4,6,9,11,15,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	3,5,14	2,4,6,9,11	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	3,5,14,16,17,18	2,4,6,9,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	3,5,14,18	2,4,6,9,11,15,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	3,5,14,16,17	2,4,6,9,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,17	2,4,6,9,11,13,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	3,5,16,18	2,4,6,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,17,18	2,4,6,9,11,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	3,5,16	2,4,6,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	3,5,14,18	2,4,6,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	3,5,14,16,17	2,4,6,9,11,13,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	3,5,14	2,4,6,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	3,5,14,16,17,18	2,4,6,9,11,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,5,12	2,4,6,9,11	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,5,12,16,17,18	2,4,6,9,11,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	3,5,12,18	2,4,6,9,11,15,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	3,5,12,16,17	2,4,6,9,11,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	3,5,12,14,17,18	2,4,6,9,11,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	3,5,12,14,16	2,4,6,9,11	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	3,5,12,14,17	2,4,6,9,11,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	3,5,12,14,16,18	2,4,6,9,11,15,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	3,5,12,18	2,4,6,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	3,5,12,16,17	2,4,6,9,11,13,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	3,5,12	2,4,6,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	3,5,12,16,17,18	2,4,6,9,11,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	3,5,12,14,17	2,4,6,9,11,13,17	2^{-1}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	3,5,12,14,16,18	2,4,6,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	3,5,12,14,17,18	2,4,6,9,11,13,15,17,18	2^{-1}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	3,5,12,14,16	2,4,6,9,11,13,15	$2^{-17.5}$

Table 0.999 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	3,5,10,18	2,4,6,9,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	3,5,10,16,17	2,4,6,9,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	3,5,10	2,4,6,9,15	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	3,5,10,16,17,18	2,4,6,9,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	3,5,10,14,17	2,4,6,9,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	3,5,10,14,16,18	2,4,6,9,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	3,5,10,14,17,18	2,4,6,9,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	3,5,10,14,16	2,4,6,9,15	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	3,5,10	2,4,6,9,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	3,5,10,16,17,18	2,4,6,9,13,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	3,5,10,18	2,4,6,9,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	3,5,10,16,17	2,4,6,9,13,15,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	3,5,10,14,17,18	2,4,6,9,13,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	3,5,10,14,16	2,4,6,9,13	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	3,5,10,14,17	2,4,6,9,13,15,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	3,5,10,14,16,18	2,4,6,9,13,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	3,5,10,12,17	2,4,6,9,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	3,5,10,12,16,18	2,4,6,9,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	3,5,10,12,17,18	2,4,6,9,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	3,5,10,12,16	2,4,6,9,15	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	3,5,10,12,14,18	2,4,6,9,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	3,5,10,12,14,16,17	2,4,6,9,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	3,5,10,12,14	2,4,6,9,15	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	3,5,10,12,14,16,17,18	2,4,6,9,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	3,5,10,12,17,18	2,4,6,9,13,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	3,5,10,12,16	2,4,6,9,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	3,5,10,12,17	2,4,6,9,13,15,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	3,5,10,12,16,18	2,4,6,9,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	3,5,10,12,14	2,4,6,9,13	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	3,5,10,12,14,16,17,18	2,4,6,9,13,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,5,10,12,14,18	2,4,6,9,13,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	3,5,10,12,14,16,17	2,4,6,9,13,15,17	2^{-23}

Table 0.1000 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	3,5,10	2,4,6,9,11	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	3,5,10,16,17,18	2,4,6,9,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	3,5,10,18	2,4,6,9,11,15,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	3,5,10,16,17	2,4,6,9,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	3,5,10,14,17,18	2,4,6,9,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	3,5,10,14,16	2,4,6,9,11	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	3,5,10,14,17	2,4,6,9,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	3,5,10,14,16,18	2,4,6,9,11,15,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	3,5,10,18	2,4,6,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	3,5,10,16,17	2,4,6,9,11,13,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	3,5,10	2,4,6,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	3,5,10,16,17,18	2,4,6,9,11,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	3,5,10,14,17	2,4,6,9,11,13,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	3,5,10,14,16,18	2,4,6,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	3,5,10,14,17,18	2,4,6,9,11,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	3,5,10,14,16	2,4,6,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	3,5,10,12,17,18	2,4,6,9,11,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	3,5,10,12,16	2,4,6,9,11	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	3,5,10,12,17	2,4,6,9,11,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	3,5,10,12,16,18	2,4,6,9,11,15,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	3,5,10,12,14	2,4,6,9,11	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	3,5,10,12,14,16,17,18	2,4,6,9,11,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	3,5,10,12,14,18	2,4,6,9,11,15,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	3,5,10,12,14,16,17	2,4,6,9,11,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	3,5,10,12,17	2,4,6,9,11,13,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	3,5,10,12,16,18	2,4,6,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	3,5,10,12,17,18	2,4,6,9,11,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	3,5,10,12,16	2,4,6,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	3,5,10,12,14,18	2,4,6,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	3,5,10,12,14,16,17	2,4,6,9,11,13,17	2^{-34}
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	3,5,10,12,14	2,4,6,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	3,5,10,12,14,16,17,18	2,4,6,9,11,13,15,17,18	2^{-34}

Table 0.1001 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	3,5	2,4,6,8	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	3,5,16,17,18	2,4,6,8,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	3,5,18	2,4,6,8,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	3,5,16,17	2,4,6,8,15,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	3,5,14,17,18	2,4,6,8,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	3,5,14,16	2,4,6,8	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	3,5,14,17	2,4,6,8,15,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	3,5,14,16,18	2,4,6,8,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	3,5,18	2,4,6,8,13,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	3,5,16,17	2,4,6,8,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	3,5	2,4,6,8,13,15	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	3,5,16,17,18	2,4,6,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	3,5,14,17	2,4,6,8,13,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	3,5,14,16,18	2,4,6,8,13,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	3,5,14,17,18	2,4,6,8,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	3,5,14,16	2,4,6,8,13,15	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	3,5,12,17,18	2,4,6,8,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	3,5,12,16	2,4,6,8	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	3,5,12,17	2,4,6,8,15,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	3,5,12,16,18	2,4,6,8,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	3,5,12,14	2,4,6,8	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	3,5,12,14,16,17,18	2,4,6,8,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	3,5,12,14,18	2,4,6,8,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	3,5,12,14,16,17	2,4,6,8,15,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	3,5,12,17	2,4,6,8,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	3,5,12,16,18	2,4,6,8,13,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	3,5,12,17,18	2,4,6,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	3,5,12,16	2,4,6,8,13,15	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	3,5,12,14,18	2,4,6,8,13,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	3,5,12,14,16,17	2,4,6,8,13,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	3,5,12,14	2,4,6,8,13,15	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,5,12,14,16,17,18	2,4,6,8,13,15,17,18	$2^{-6.5}$

Table 0.1002 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	3,5,18	2,4,6,8,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	3,5,16,17	2,4,6,8,11,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	3,5	2,4,6,8,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	3,5,16,17,18	2,4,6,8,11,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	3,5,14,17	2,4,6,8,11,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	3,5,14,16,18	2,4,6,8,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	3,5,14,17,18	2,4,6,8,11,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	3,5,14,16	2,4,6,8,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	3,5	2,4,6,8,11,13	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	3,5,16,17,18	2,4,6,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	3,5,18	2,4,6,8,11,13,15,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	3,5,16,17	2,4,6,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	3,5,14,17,18	2,4,6,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	3,5,14,16	2,4,6,8,11,13	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	3,5,14,17	2,4,6,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	3,5,14,16,18	2,4,6,8,11,13,15,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	3,5,12,17	2,4,6,8,11,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	3,5,12,16,18	2,4,6,8,11,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	3,5,12,17,18	2,4,6,8,11,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	3,5,12,16	2,4,6,8,11,15	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	3,5,12,14,18	2,4,6,8,11,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	3,5,12,14,16,17	2,4,6,8,11,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	3,5,12,14	2,4,6,8,11,15	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	3,5,12,14,16,17,18	2,4,6,8,11,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	3,5,12,17,18	2,4,6,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	3,5,12,16	2,4,6,8,11,13	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	3,5,12,17	2,4,6,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	3,5,12,16,18	2,4,6,8,11,13,15,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	3,5,12,14	2,4,6,8,11,13	2^{-34}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	3,5,12,14,16,17,18	2,4,6,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	3,5,12,14,18	2,4,6,8,11,13,15,18	2^{-34}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	3,5,12,14,16,17	2,4,6,8,11,13,15,17	$2^{-17.5}$

Table 0.1003 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	3,5,10,17,18	2,4,6,8,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	3,5,10,16	2,4,6,8	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	3,5,10,17	2,4,6,8,15,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	3,5,10,16,18	2,4,6,8,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	3,5,10,14	2,4,6,8	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	3,5,10,14,16,17,18	2,4,6,8,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	3,5,10,14,18	2,4,6,8,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	3,5,10,14,16,17	2,4,6,8,15,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	3,5,10,17	2,4,6,8,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	3,5,10,16,18	2,4,6,8,13,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	3,5,10,17,18	2,4,6,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	3,5,10,16	2,4,6,8,13,15	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	3,5,10,14,18	2,4,6,8,13,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	3,5,10,14,16,17	2,4,6,8,13,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	3,5,10,14	2,4,6,8,13,15	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	3,5,10,14,16,17,18	2,4,6,8,13,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	3,5,10,12	2,4,6,8	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	3,5,10,12,16,17,18	2,4,6,8,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	3,5,10,12,18	2,4,6,8,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	3,5,10,12,16,17	2,4,6,8,15,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	3,5,10,12,14,17,18	2,4,6,8,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	3,5,10,12,14,16	2,4,6,8	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	3,5,10,12,14,17	2,4,6,8,15,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,5,10,12,14,16,18	2,4,6,8,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	3,5,10,12,18	2,4,6,8,13,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	3,5,10,12,16,17	2,4,6,8,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	3,5,10,12	2,4,6,8,13,15	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	3,5,10,12,16,17,18	2,4,6,8,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	3,5,10,12,14,17	2,4,6,8,13,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,10,12,14,16,18	2,4,6,8,13,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	3,5,10,12,14,17,18	2,4,6,8,13,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,10,12,14,16	2,4,6,8,13,15	2^{-12}

Table 0.1004 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	3,5,10,17	2,4,6,8,11,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	3,5,10,16,18	2,4,6,8,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	3,5,10,17,18	2,4,6,8,11,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	3,5,10,16	2,4,6,8,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	3,5,10,14,18	2,4,6,8,11,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	3,5,10,14,16,17	2,4,6,8,11,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	3,5,10,14	2,4,6,8,11,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	3,5,10,14,16,17,18	2,4,6,8,11,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	3,5,10,17,18	2,4,6,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,10,16	2,4,6,8,11,13	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	3,5,10,17	2,4,6,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,10,16,18	2,4,6,8,11,13,15,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	3,5,10,14	2,4,6,8,11,13	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	3,5,10,14,16,17,18	2,4,6,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	3,5,10,14,18	2,4,6,8,11,13,15,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	3,5,10,14,16,17	2,4,6,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,5,10,12,18	2,4,6,8,11,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,5,10,12,16,17	2,4,6,8,11,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	3,5,10,12	2,4,6,8,11,15	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,5,10,12,16,17,18	2,4,6,8,11,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	3,5,10,12,14,17	2,4,6,8,11,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	3,5,10,12,14,16,18	2,4,6,8,11,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	3,5,10,12,14,17,18	2,4,6,8,11,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	3,5,10,12,14,16	2,4,6,8,11,15	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	3,5,10,12	2,4,6,8,11,13	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	3,5,10,12,16,17,18	2,4,6,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	3,5,10,12,18	2,4,6,8,11,13,15,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	3,5,10,12,16,17	2,4,6,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	3,5,10,12,14,17,18	2,4,6,8,11,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	3,5,10,12,14,16	2,4,6,8,11,13	2^{-1}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	3,5,10,12,14,17	2,4,6,8,11,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	3,5,10,12,14,16,18	2,4,6,8,11,13,15,18	2^{-1}

Table 0.1005 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	3,5,18	2,4,6,8,9,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,16,17	2,4,6,8,9,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	3,5	2,4,6,8,9,15	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,16,17,18	2,4,6,8,9,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	3,5,14,17	2,4,6,8,9,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	3,5,14,16,18	2,4,6,8,9,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	3,5,14,17,18	2,4,6,8,9,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	3,5,14,16	2,4,6,8,9,15	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	3,5	2,4,6,8,9,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	3,5,16,17,18	2,4,6,8,9,13,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	3,5,18	2,4,6,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	3,5,16,17	2,4,6,8,9,13,15,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,14,17,18	2,4,6,8,9,13,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	3,5,14,16	2,4,6,8,9,13	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,14,17	2,4,6,8,9,13,15,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	3,5,14,16,18	2,4,6,8,9,13,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	3,5,12,17	2,4,6,8,9,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	3,5,12,16,18	2,4,6,8,9,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	3,5,12,17,18	2,4,6,8,9,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	3,5,12,16	2,4,6,8,9,15	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	3,5,12,14,18	2,4,6,8,9,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	3,5,12,14,16,17	2,4,6,8,9,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	3,5,12,14	2,4,6,8,9,15	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	3,5,12,14,16,17,18	2,4,6,8,9,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	3,5,12,17,18	2,4,6,8,9,13,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	3,5,12,16	2,4,6,8,9,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	3,5,12,17	2,4,6,8,9,13,15,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	3,5,12,16,18	2,4,6,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	3,5,12,14	2,4,6,8,9,13	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	3,5,12,14,16,17,18	2,4,6,8,9,13,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	3,5,12,14,18	2,4,6,8,9,13,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	3,5,12,14,16,17	2,4,6,8,9,13,15,17	2^{-12}

Table 0.1006 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	3,5	2,4,6,8,9,11	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	3,5,16,17,18	2,4,6,8,9,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	3,5,18	2,4,6,8,9,11,15,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	3,5,16,17	2,4,6,8,9,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	3,5,14,17,18	2,4,6,8,9,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,5,14,16	2,4,6,8,9,11	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	3,5,14,17	2,4,6,8,9,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	3,5,14,16,18	2,4,6,8,9,11,15,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	3,5,18	2,4,6,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	3,5,16,17	2,4,6,8,9,11,13,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,5	2,4,6,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	3,5,16,17,18	2,4,6,8,9,11,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	3,5,14,17	2,4,6,8,9,11,13,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	3,5,14,16,18	2,4,6,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	3,5,14,17,18	2,4,6,8,9,11,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	3,5,14,16	2,4,6,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	3,5,12,17,18	2,4,6,8,9,11,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	3,5,12,16	2,4,6,8,9,11	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	3,5,12,17	2,4,6,8,9,11,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	3,5,12,16,18	2,4,6,8,9,11,15,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	3,5,12,14	2,4,6,8,9,11	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	3,5,12,14,16,17,18	2,4,6,8,9,11,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,5,12,14,18	2,4,6,8,9,11,15,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	3,5,12,14,16,17	2,4,6,8,9,11,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	3,5,12,17	2,4,6,8,9,11,13,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	3,5,12,16,18	2,4,6,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	3,5,12,17,18	2,4,6,8,9,11,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	3,5,12,16	2,4,6,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,5,12,14,18	2,4,6,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	3,5,12,14,16,17	2,4,6,8,9,11,13,17	2^{-1}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,5,12,14	2,4,6,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	3,5,12,14,16,17,18	2,4,6,8,9,11,13,15,17,18	2^{-1}

Table 0.1007 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	3,5,10,17	2,4,6,8,9,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	3,5,10,16,18	2,4,6,8,9,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	3,5,10,17,18	2,4,6,8,9,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	3,5,10,16	2,4,6,8,9,15	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	3,5,10,14,18	2,4,6,8,9,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5,10,14,16,17	2,4,6,8,9,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	3,5,10,14	2,4,6,8,9,15	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5,10,14,16,17,18	2,4,6,8,9,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	3,5,10,17,18	2,4,6,8,9,13,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,10,16	2,4,6,8,9,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	3,5,10,17	2,4,6,8,9,13,15,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,10,16,18	2,4,6,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	3,5,10,14	2,4,6,8,9,13	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	3,5,10,14,16,17,18	2,4,6,8,9,13,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	3,5,10,14,18	2,4,6,8,9,13,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	3,5,10,14,16,17	2,4,6,8,9,13,15,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	3,5,10,12,18	2,4,6,8,9,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	3,5,10,12,16,17	2,4,6,8,9,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	3,5,10,12	2,4,6,8,9,15	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	3,5,10,12,16,17,18	2,4,6,8,9,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	3,5,10,12,14,17	2,4,6,8,9,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	3,5,10,12,14,16,18	2,4,6,8,9,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	3,5,10,12,14,17,18	2,4,6,8,9,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	3,5,10,12,14,16	2,4,6,8,9,15	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	3,5,10,12	2,4,6,8,9,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	3,5,10,12,16,17,18	2,4,6,8,9,13,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	3,5,10,12,18	2,4,6,8,9,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	3,5,10,12,16,17	2,4,6,8,9,13,15,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	3,5,10,12,14,17,18	2,4,6,8,9,13,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	3,5,10,12,14,16	2,4,6,8,9,13	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	3,5,10,12,14,17	2,4,6,8,9,13,15,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	3,5,10,12,14,16,18	2,4,6,8,9,13,15,18	$2^{-6.5}$

Table 0.1008 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	3,5,10,17,18	2,4,6,8,9,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	3,5,10,16	2,4,6,8,9,11	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	3,5,10,17	2,4,6,8,9,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	3,5,10,16,18	2,4,6,8,9,11,15,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	3,5,10,14	2,4,6,8,9,11	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	3,5,10,14,16,17,18	2,4,6,8,9,11,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	3,5,10,14,18	2,4,6,8,9,11,15,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	3,5,10,14,16,17	2,4,6,8,9,11,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	3,5,10,17	2,4,6,8,9,11,13,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	3,5,10,16,18	2,4,6,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	3,5,10,17,18	2,4,6,8,9,11,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	3,5,10,16	2,4,6,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,10,14,18	2,4,6,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	3,5,10,14,16,17	2,4,6,8,9,11,13,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,10,14	2,4,6,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	3,5,10,14,16,17,18	2,4,6,8,9,11,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	3,5,10,12	2,4,6,8,9,11	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	3,5,10,12,16,17,18	2,4,6,8,9,11,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	3,5,10,12,18	2,4,6,8,9,11,15,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	3,5,10,12,16,17	2,4,6,8,9,11,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	3,5,10,12,14,17,18	2,4,6,8,9,11,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,10,12,14,16	2,4,6,8,9,11	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	3,5,10,12,14,17	2,4,6,8,9,11,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	3,5,10,12,14,16,18	2,4,6,8,9,11,15,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	3,5,10,12,18	2,4,6,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	3,5,10,12,16,17	2,4,6,8,9,11,13,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	3,5,10,12	2,4,6,8,9,11,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	3,5,10,12,16,17,18	2,4,6,8,9,11,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	3,5,10,12,14,17	2,4,6,8,9,11,13,17	2^{-34}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	3,5,10,12,14,16,18	2,4,6,8,9,11,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	3,5,10,12,14,17,18	2,4,6,8,9,11,13,15,17,18	2^{-34}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	3,5,10,12,14,16	2,4,6,8,9,11,13,15	$2^{-17.5}$

Table 0.1009 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	3,5,7,17	2,4,6,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	3,5,7,16,18	2,4,6,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	3,5,7,17,18	2,4,6,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	3,5,7,16	2,4,6,15	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	3,5,7,14,18	2,4,6,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	3,5,7,14,16,17	2,4,6,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	3,5,7,14	2,4,6,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	3,5,7,14,16,17,18	2,4,6,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,7,17,18	2,4,6,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	3,5,7,16	2,4,6,13	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,7,17	2,4,6,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	3,5,7,16,18	2,4,6,13,15,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	3,5,7,14	2,4,6,13	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	3,5,7,14,16,17,18	2,4,6,13,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	3,5,7,14,18	2,4,6,13,15,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	3,5,7,14,16,17	2,4,6,13,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	3,5,7,12,18	2,4,6,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	3,5,7,12,16,17	2,4,6,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,5,7,12	2,4,6,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,5,7,12,16,17,18	2,4,6,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	3,5,7,12,14,17	2,4,6,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	3,5,7,12,14,16,18	2,4,6,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	3,5,7,12,14,17,18	2,4,6,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	3,5,7,12,14,16	2,4,6,15	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	3,5,7,12	2,4,6,13	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	3,5,7,12,16,17,18	2,4,6,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	3,5,7,12,18	2,4,6,13,15,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	3,5,7,12,16,17	2,4,6,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	3,5,7,12,14,17,18	2,4,6,13,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	3,5,7,12,14,16	2,4,6,13	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	3,5,7,12,14,17	2,4,6,13,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	3,5,7,12,14,16,18	2,4,6,13,15,18	2^{-23}

Table 0.1010 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	3,5,7,17,18	2,4,6,11,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	3,5,7,16	2,4,6,11	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,5,7,17	2,4,6,11,15,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	3,5,7,16,18	2,4,6,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	3,5,7,14	2,4,6,11	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	3,5,7,14,16,17,18	2,4,6,11,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	3,5,7,14,18	2,4,6,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	3,5,7,14,16,17	2,4,6,11,15,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	3,5,7,17	2,4,6,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	3,5,7,16,18	2,4,6,11,13,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	3,5,7,17,18	2,4,6,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	3,5,7,16	2,4,6,11,13,15	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	3,5,7,14,18	2,4,6,11,13,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	3,5,7,14,16,17	2,4,6,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	3,5,7,14	2,4,6,11,13,15	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	3,5,7,14,16,17,18	2,4,6,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	3,5,7,12	2,4,6,11	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	3,5,7,12,16,17,18	2,4,6,11,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	3,5,7,12,18	2,4,6,11,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	3,5,7,12,16,17	2,4,6,11,15,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,5,7,12,14,17,18	2,4,6,11,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	3,5,7,12,14,16	2,4,6,11	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	3,5,7,12,14,17	2,4,6,11,15,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	3,5,7,12,14,16,18	2,4,6,11,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	3,5,7,12,18	2,4,6,11,13,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	3,5,7,12,16,17	2,4,6,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	3,5,7,12	2,4,6,11,13,15	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	3,5,7,12,16,17,18	2,4,6,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,7,12,14,17	2,4,6,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	3,5,7,12,14,16,18	2,4,6,11,13,18	2^{-34}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,7,12,14,17,18	2,4,6,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	3,5,7,12,14,16	2,4,6,11,13,15	2^{-34}

Table 0.1011 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	3,5,7,10,18	2,4,6,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	3,5,7,10,16,17	2,4,6,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	3,5,7,10	2,4,6,15	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	3,5,7,10,16,17,18	2,4,6,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	3,5,7,10,14,17	2,4,6,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	3,5,7,10,14,16,18	2,4,6,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	3,5,7,10,14,17,18	2,4,6,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	3,5,7,10,14,16	2,4,6,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	3,5,7,10	2,4,6,13	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	3,5,7,10,16,17,18	2,4,6,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	3,5,7,10,18	2,4,6,13,15,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	3,5,7,10,16,17	2,4,6,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	3,5,7,10,14,17,18	2,4,6,13,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	3,5,7,10,14,16	2,4,6,13	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	3,5,7,10,14,17	2,4,6,13,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	3,5,7,10,14,16,18	2,4,6,13,15,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	3,5,7,10,12,17	2,4,6,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	3,5,7,10,12,16,18	2,4,6,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	3,5,7,10,12,17,18	2,4,6,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	3,5,7,10,12,16	2,4,6,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	3,5,7,10,12,14,18	2,4,6,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	3,5,7,10,12,14,16,17	2,4,6,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	3,5,7,10,12,14	2,4,6,15	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,7,10,12,14,16,17,18	2,4,6,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	3,5,7,10,12,17,18	2,4,6,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	3,5,7,10,12,16	2,4,6,13	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	3,5,7,10,12,17	2,4,6,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	3,5,7,10,12,16,18	2,4,6,13,15,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	3,5,7,10,12,14	2,4,6,13	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	3,5,7,10,12,14,16,17,18	2,4,6,13,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	3,5,7,10,12,14,18	2,4,6,13,15,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	3,5,7,10,12,14,16,17	2,4,6,13,15,17	$2^{-28.5}$

Table 0.1012 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	3,5,7,10	2,4,6,11	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	3,5,7,10,16,17,18	2,4,6,11,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	3,5,7,10,18	2,4,6,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	3,5,7,10,16,17	2,4,6,11,15,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	3,5,7,10,14,17,18	2,4,6,11,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	3,5,7,10,14,16	2,4,6,11	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	3,5,7,10,14,17	2,4,6,11,15,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	3,5,7,10,14,16,18	2,4,6,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	3,5,7,10,18	2,4,6,11,13,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	3,5,7,10,16,17	2,4,6,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	3,5,7,10	2,4,6,11,13,15	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	3,5,7,10,16,17,18	2,4,6,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	3,5,7,10,14,17	2,4,6,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	3,5,7,10,14,16,18	2,4,6,11,13,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	3,5,7,10,14,17,18	2,4,6,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	3,5,7,10,14,16	2,4,6,11,13,15	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	3,5,7,10,12,17,18	2,4,6,11,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	3,5,7,10,12,16	2,4,6,11	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	3,5,7,10,12,17	2,4,6,11,15,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	3,5,7,10,12,16,18	2,4,6,11,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	3,5,7,10,12,14	2,4,6,11	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	3,5,7,10,12,14,16,17,18	2,4,6,11,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	3,5,7,10,12,14,18	2,4,6,11,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	3,5,7,10,12,14,16,17	2,4,6,11,15,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	3,5,7,10,12,17	2,4,6,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	3,5,7,10,12,16,18	2,4,6,11,13,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	3,5,7,10,12,17,18	2,4,6,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	3,5,7,10,12,16	2,4,6,11,13,15	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,5,7,10,12,14,18	2,4,6,11,13,18	2^{-1}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	3,5,7,10,12,14,16,17	2,4,6,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	3,5,7,10,12,14	2,4,6,11,13,15	2^{-1}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	3,5,7,10,12,14,16,17,18	2,4,6,11,13,15,17,18	$2^{-17.5}$

Table 0.1013 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	3,5,7,17,18	2,4,6,9,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,16	2,4,6,9	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	3,5,7,17	2,4,6,9,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,16,18	2,4,6,9,15,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,14	2,4,6,9	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	3,5,7,14,16,17,18	2,4,6,9,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,14,18	2,4,6,9,15,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	3,5,7,14,16,17	2,4,6,9,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	3,5,7,17	2,4,6,9,13,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	3,5,7,16,18	2,4,6,9,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	3,5,7,17,18	2,4,6,9,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	3,5,7,16	2,4,6,9,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	3,5,7,14,18	2,4,6,9,13,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,7,14,16,17	2,4,6,9,13,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	3,5,7,14	2,4,6,9,13,15	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,7,14,16,17,18	2,4,6,9,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	3,5,7,12	2,4,6,9	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	3,5,7,12,16,17,18	2,4,6,9,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	3,5,7,12,18	2,4,6,9,15,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	3,5,7,12,16,17	2,4,6,9,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	3,5,7,12,14,17,18	2,4,6,9,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	3,5,7,12,14,16	2,4,6,9	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,5,7,12,14,17	2,4,6,9,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	3,5,7,12,14,16,18	2,4,6,9,15,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	3,5,7,12,18	2,4,6,9,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	3,5,7,12,16,17	2,4,6,9,13,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	3,5,7,12	2,4,6,9,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	3,5,7,12,16,17,18	2,4,6,9,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	3,5,7,12,14,17	2,4,6,9,13,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	3,5,7,12,14,16,18	2,4,6,9,13,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	3,5,7,12,14,17,18	2,4,6,9,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	3,5,7,12,14,16	2,4,6,9,13,15	$2^{-28.5}$

Table 0.1014 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	3,5,7,17	2,4,6,9,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	3,5,7,16,18	2,4,6,9,11,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	3,5,7,17,18	2,4,6,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	3,5,7,16	2,4,6,9,11,15	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5,7,14,18	2,4,6,9,11,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	3,5,7,14,16,17	2,4,6,9,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5,7,14	2,4,6,9,11,15	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	3,5,7,14,16,17,18	2,4,6,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,7,17,18	2,4,6,9,11,13,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	3,5,7,16	2,4,6,9,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,7,17	2,4,6,9,11,13,15,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	3,5,7,16,18	2,4,6,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	3,5,7,14	2,4,6,9,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	3,5,7,14,16,17,18	2,4,6,9,11,13,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	3,5,7,14,18	2,4,6,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	3,5,7,14,16,17	2,4,6,9,11,13,15,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	3,5,7,12,18	2,4,6,9,11,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	3,5,7,12,16,17	2,4,6,9,11,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	3,5,7,12	2,4,6,9,11,15	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	3,5,7,12,16,17,18	2,4,6,9,11,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	3,5,7,12,14,17	2,4,6,9,11,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	3,5,7,12,14,16,18	2,4,6,9,11,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	3,5,7,12,14,17,18	2,4,6,9,11,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	3,5,7,12,14,16	2,4,6,9,11,15	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	3,5,7,12	2,4,6,9,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	3,5,7,12,16,17,18	2,4,6,9,11,13,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	3,5,7,12,18	2,4,6,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	3,5,7,12,16,17	2,4,6,9,11,13,15,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	3,5,7,12,14,17,18	2,4,6,9,11,13,17,18	2^{-1}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	3,5,7,12,14,16	2,4,6,9,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	3,5,7,12,14,17	2,4,6,9,11,13,15,17	2^{-1}
$(0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	3,5,7,12,14,16,18	2,4,6,9,11,13,15,18	$2^{-17.5}$

Table 0.1015 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	3,5,7,10	2,4,6,9	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	3,5,7,10,16,17,18	2,4,6,9,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	3,5,7,10,18	2,4,6,9,15,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	3,5,7,10,16,17	2,4,6,9,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	3,5,7,10,14,17,18	2,4,6,9,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	3,5,7,10,14,16	2,4,6,9	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,5,7,10,14,17	2,4,6,9,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	3,5,7,10,14,16,18	2,4,6,9,15,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	3,5,7,10,18	2,4,6,9,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	3,5,7,10,16,17	2,4,6,9,13,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	3,5,7,10	2,4,6,9,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	3,5,7,10,16,17,18	2,4,6,9,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	3,5,7,10,14,17	2,4,6,9,13,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	3,5,7,10,14,16,18	2,4,6,9,13,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	3,5,7,10,14,17,18	2,4,6,9,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	3,5,7,10,14,16	2,4,6,9,13,15	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,10,12,17,18	2,4,6,9,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	3,5,7,10,12,16	2,4,6,9	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,10,12,17	2,4,6,9,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	3,5,7,10,12,16,18	2,4,6,9,15,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	3,5,7,10,12,14	2,4,6,9	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,5,7,10,12,14,16,17,18	2,4,6,9,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	3,5,7,10,12,14,18	2,4,6,9,15,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	3,5,7,10,12,14,16,17	2,4,6,9,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	3,5,7,10,12,17	2,4,6,9,13,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	3,5,7,10,12,16,18	2,4,6,9,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	3,5,7,10,12,17,18	2,4,6,9,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	3,5,7,10,12,16	2,4,6,9,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	3,5,7,10,12,14,18	2,4,6,9,13,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	3,5,7,10,12,14,16,17	2,4,6,9,13,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	3,5,7,10,12,14	2,4,6,9,13,15	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	3,5,7,10,12,14,16,17,18	2,4,6,9,13,15,17,18	2^{-23}

Table 0.1016 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,7,10,18	2,4,6,9,11,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	3,5,7,10,16,17	2,4,6,9,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,7,10	2,4,6,9,11,15	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	3,5,7,10,16,17,18	2,4,6,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	3,5,7,10,14,17	2,4,6,9,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	3,5,7,10,14,16,18	2,4,6,9,11,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	3,5,7,10,14,17,18	2,4,6,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	3,5,7,10,14,16	2,4,6,9,11,15	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	3,5,7,10	2,4,6,9,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	3,5,7,10,16,17,18	2,4,6,9,11,13,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	3,5,7,10,18	2,4,6,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	3,5,7,10,16,17	2,4,6,9,11,13,15,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	3,5,7,10,14,17,18	2,4,6,9,11,13,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,7,10,14,16	2,4,6,9,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	3,5,7,10,14,17	2,4,6,9,11,13,15,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,7,10,14,16,18	2,4,6,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	3,5,7,10,12,17	2,4,6,9,11,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	3,5,7,10,12,16,18	2,4,6,9,11,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	3,5,7,10,12,17,18	2,4,6,9,11,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	3,5,7,10,12,16	2,4,6,9,11,15	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	3,5,7,10,12,14,18	2,4,6,9,11,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	3,5,7,10,12,14,16,17	2,4,6,9,11,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	3,5,7,10,12,14	2,4,6,9,11,15	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	3,5,7,10,12,14,16,17,18	2,4,6,9,11,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	3,5,7,10,12,17,18	2,4,6,9,11,13,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	3,5,7,10,12,16	2,4,6,9,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	3,5,7,10,12,17	2,4,6,9,11,13,15,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	3,5,7,10,12,16,18	2,4,6,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	3,5,7,10,12,14	2,4,6,9,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	3,5,7,10,12,14,16,17,18	2,4,6,9,11,13,17,18	2^{-34}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	3,5,7,10,12,14,18	2,4,6,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	3,5,7,10,12,14,16,17	2,4,6,9,11,13,15,17	2^{-34}

Table 0.1017 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	3,5,7,18	2,4,6,8,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	3,5,7,16,17	2,4,6,8,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	3,5,7	2,4,6,8,15	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	3,5,7,16,17,18	2,4,6,8,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	3,5,7,14,17	2,4,6,8,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	3,5,7,14,16,18	2,4,6,8,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	3,5,7,14,17,18	2,4,6,8,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	3,5,7,14,16	2,4,6,8,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	3,5,7	2,4,6,8,13	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	3,5,7,16,17,18	2,4,6,8,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	3,5,7,18	2,4,6,8,13,15,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	3,5,7,16,17	2,4,6,8,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	3,5,7,14,17,18	2,4,6,8,13,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	3,5,7,14,16	2,4,6,8,13	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	3,5,7,14,17	2,4,6,8,13,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	3,5,7,14,16,18	2,4,6,8,13,15,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	3,5,7,12,17	2,4,6,8,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,12,16,18	2,4,6,8,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	3,5,7,12,17,18	2,4,6,8,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	3,5,7,12,16	2,4,6,8,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	3,5,7,12,14,18	2,4,6,8,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	3,5,7,12,14,16,17	2,4,6,8,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	3,5,7,12,14	2,4,6,8,15	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	3,5,7,12,14,16,17,18	2,4,6,8,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	3,5,7,12,17,18	2,4,6,8,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	3,5,7,12,16	2,4,6,8,13	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	3,5,7,12,17	2,4,6,8,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	3,5,7,12,16,18	2,4,6,8,13,15,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,5,7,12,14	2,4,6,8,13	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	3,5,7,12,14,16,17,18	2,4,6,8,13,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	3,5,7,12,14,18	2,4,6,8,13,15,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	3,5,7,12,14,16,17	2,4,6,8,13,15,17	$2^{-6.5}$

Table 0.1018 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	3,5,7	2,4,6,8,11	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,7,16,17,18	2,4,6,8,11,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	3,5,7,18	2,4,6,8,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	3,5,7,16,17	2,4,6,8,11,15,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	3,5,7,14,17,18	2,4,6,8,11,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	3,5,7,14,16	2,4,6,8,11	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	3,5,7,14,17	2,4,6,8,11,15,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	3,5,7,14,16,18	2,4,6,8,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	3,5,7,18	2,4,6,8,11,13,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	3,5,7,16,17	2,4,6,8,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	3,5,7	2,4,6,8,11,13,15	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	3,5,7,16,17,18	2,4,6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,7,14,17	2,4,6,8,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	3,5,7,14,16,18	2,4,6,8,11,13,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	3,5,7,14,17,18	2,4,6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	3,5,7,14,16	2,4,6,8,11,13,15	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	3,5,7,12,17,18	2,4,6,8,11,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	3,5,7,12,16	2,4,6,8,11	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	3,5,7,12,17	2,4,6,8,11,15,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	3,5,7,12,16,18	2,4,6,8,11,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	3,5,7,12,14	2,4,6,8,11	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	3,5,7,12,14,16,17,18	2,4,6,8,11,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	3,5,7,12,14,18	2,4,6,8,11,15,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	3,5,7,12,14,16,17	2,4,6,8,11,15,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	3,5,7,12,17	2,4,6,8,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	3,5,7,12,16,18	2,4,6,8,11,13,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	3,5,7,12,17,18	2,4,6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	3,5,7,12,16	2,4,6,8,11,13,15	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	3,5,7,12,14,18	2,4,6,8,11,13,18	2^{-34}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	3,5,7,12,14,16,17	2,4,6,8,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	3,5,7,12,14	2,4,6,8,11,13,15	2^{-34}
$(0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	3,5,7,12,14,16,17,18	2,4,6,8,11,13,15,17,18	$2^{-17.5}$

Table 0.1019 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,10,17	2,4,6,8,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	3,5,7,10,16,18	2,4,6,8,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	3,5,7,10,17,18	2,4,6,8,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	3,5,7,10,16	2,4,6,8,15	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	3,5,7,10,14,18	2,4,6,8,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,10,14,16,17	2,4,6,8,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	3,5,7,10,14	2,4,6,8,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	3,5,7,10,14,16,17,18	2,4,6,8,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	3,5,7,10,17,18	2,4,6,8,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	3,5,7,10,16	2,4,6,8,13	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	3,5,7,10,17	2,4,6,8,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	3,5,7,10,16,18	2,4,6,8,13,15,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,7,10,14	2,4,6,8,13	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	3,5,7,10,14,16,17,18	2,4,6,8,13,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	3,5,7,10,14,18	2,4,6,8,13,15,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	3,5,7,10,14,16,17	2,4,6,8,13,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	3,5,7,10,12,18	2,4,6,8,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	3,5,7,10,12,16,17	2,4,6,8,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	3,5,7,10,12	2,4,6,8,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	3,5,7,10,12,16,17,18	2,4,6,8,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	3,5,7,10,12,14,17	2,4,6,8,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	3,5,7,10,12,14,16,18	2,4,6,8,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	3,5,7,10,12,14,17,18	2,4,6,8,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	3,5,7,10,12,14,16	2,4,6,8,15	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	3,5,7,10,12	2,4,6,8,13	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	3,5,7,10,12,16,17,18	2,4,6,8,13,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	3,5,7,10,12,18	2,4,6,8,13,15,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	3,5,7,10,12,16,17	2,4,6,8,13,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	3,5,7,10,12,14,17,18	2,4,6,8,13,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	3,5,7,10,12,14,16	2,4,6,8,13	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	3,5,7,10,12,14,17	2,4,6,8,13,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	3,5,7,10,12,14,16,18	2,4,6,8,13,15,18	2^{-12}

Table 0.1020 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	3,5,7,10,17,18	2,4,6,8,11,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	3,5,7,10,16	2,4,6,8,11	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	3,5,7,10,17	2,4,6,8,11,15,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	3,5,7,10,16,18	2,4,6,8,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	3,5,7,10,14	2,4,6,8,11	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5,7,10,14,16,17,18	2,4,6,8,11,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	3,5,7,10,14,18	2,4,6,8,11,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	3,5,7,10,14,16,17	2,4,6,8,11,15,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	3,5,7,10,17	2,4,6,8,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	3,5,7,10,16,18	2,4,6,8,11,13,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	3,5,7,10,17,18	2,4,6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	3,5,7,10,16	2,4,6,8,11,13,15	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	3,5,7,10,14,18	2,4,6,8,11,13,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	3,5,7,10,14,16,17	2,4,6,8,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	3,5,7,10,14	2,4,6,8,11,13,15	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	3,5,7,10,14,16,17,18	2,4,6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	3,5,7,10,12	2,4,6,8,11	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	3,5,7,10,12,16,17,18	2,4,6,8,11,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	3,5,7,10,12,18	2,4,6,8,11,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	3,5,7,10,12,16,17	2,4,6,8,11,15,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	3,5,7,10,12,14,17,18	2,4,6,8,11,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	3,5,7,10,12,14,16	2,4,6,8,11	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	3,5,7,10,12,14,17	2,4,6,8,11,15,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	3,5,7,10,12,14,16,18	2,4,6,8,11,15,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	3,5,7,10,12,18	2,4,6,8,11,13,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	3,5,7,10,12,16,17	2,4,6,8,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	3,5,7,10,12	2,4,6,8,11,13,15	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	3,5,7,10,12,16,17,18	2,4,6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	3,5,7,10,12,14,17	2,4,6,8,11,13,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	3,5,7,10,12,14,16,18	2,4,6,8,11,13,18	2^{-1}
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	3,5,7,10,12,14,17,18	2,4,6,8,11,13,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	3,5,7,10,12,14,16	2,4,6,8,11,13,15	2^{-1}

Table 0.1021 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	3,5,7	2,4,6,8,9	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	3,5,7,16,17,18	2,4,6,8,9,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	3,5,7,18	2,4,6,8,9,15,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	3,5,7,16,17	2,4,6,8,9,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	3,5,7,14,17,18	2,4,6,8,9,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	3,5,7,14,16	2,4,6,8,9	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	3,5,7,14,17	2,4,6,8,9,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	3,5,7,14,16,18	2,4,6,8,9,15,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	3,5,7,18	2,4,6,8,9,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	3,5,7,16,17	2,4,6,8,9,13,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	3,5,7	2,4,6,8,9,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	3,5,7,16,17,18	2,4,6,8,9,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	3,5,7,14,17	2,4,6,8,9,13,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	3,5,7,14,16,18	2,4,6,8,9,13,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	3,5,7,14,17,18	2,4,6,8,9,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	3,5,7,14,16	2,4,6,8,9,13,15	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	3,5,7,12,17,18	2,4,6,8,9,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	3,5,7,12,16	2,4,6,8,9	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	3,5,7,12,17	2,4,6,8,9,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	3,5,7,12,16,18	2,4,6,8,9,15,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	3,5,7,12,14	2,4,6,8,9	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	3,5,7,12,14,16,17,18	2,4,6,8,9,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	3,5,7,12,14,18	2,4,6,8,9,15,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	3,5,7,12,14,16,17	2,4,6,8,9,15,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	3,5,7,12,17	2,4,6,8,9,13,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	3,5,7,12,16,18	2,4,6,8,9,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	3,5,7,12,17,18	2,4,6,8,9,13,15,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	3,5,7,12,16	2,4,6,8,9,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	3,5,7,12,14,18	2,4,6,8,9,13,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	3,5,7,12,14,16,17	2,4,6,8,9,13,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	3,5,7,12,14	2,4,6,8,9,13,15	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	3,5,7,12,14,16,17,18	2,4,6,8,9,13,15,17,18	2^{-12}

Table 0.1022 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	3,5,7,18	2,4,6,8,9,11,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	3,5,7,16,17	2,4,6,8,9,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	3,5,7	2,4,6,8,9,11,15	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	3,5,7,16,17,18	2,4,6,8,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	3,5,7,14,17	2,4,6,8,9,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	3,5,7,14,16,18	2,4,6,8,9,11,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	3,5,7,14,17,18	2,4,6,8,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	3,5,7,14,16	2,4,6,8,9,11,15	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	3,5,7	2,4,6,8,9,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	3,5,7,16,17,18	2,4,6,8,9,11,13,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	3,5,7,18	2,4,6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	3,5,7,16,17	2,4,6,8,9,11,13,15,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	3,5,7,14,17,18	2,4,6,8,9,11,13,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	3,5,7,14,16	2,4,6,8,9,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	3,5,7,14,17	2,4,6,8,9,11,13,15,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	3,5,7,14,16,18	2,4,6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	3,5,7,12,17	2,4,6,8,9,11,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	3,5,7,12,16,18	2,4,6,8,9,11,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	3,5,7,12,17,18	2,4,6,8,9,11,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	3,5,7,12,16	2,4,6,8,9,11,15	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	3,5,7,12,14,18	2,4,6,8,9,11,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	3,5,7,12,14,16,17	2,4,6,8,9,11,17	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	3,5,7,12,14	2,4,6,8,9,11,15	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	3,5,7,12,14,16,17,18	2,4,6,8,9,11,15,17,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	3,5,7,12,17,18	2,4,6,8,9,11,13,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	3,5,7,12,16	2,4,6,8,9,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	3,5,7,12,17	2,4,6,8,9,11,13,15,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	3,5,7,12,16,18	2,4,6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	3,5,7,12,14	2,4,6,8,9,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	3,5,7,12,14,16,17,18	2,4,6,8,9,11,13,17,18	2^{-1}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	3,5,7,12,14,18	2,4,6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	3,5,7,12,14,16,17	2,4,6,8,9,11,13,15,17	2^{-1}

Table 0.1023 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	3,5,7,10,17,18	2,4,6,8,9,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	3,5,7,10,16	2,4,6,8,9	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	3,5,7,10,17	2,4,6,8,9,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	3,5,7,10,16,18	2,4,6,8,9,15,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	3,5,7,10,14	2,4,6,8,9	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	3,5,7,10,14,16,17,18	2,4,6,8,9,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	3,5,7,10,14,18	2,4,6,8,9,15,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	3,5,7,10,14,16,17	2,4,6,8,9,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	3,5,7,10,17	2,4,6,8,9,13,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,7,10,16,18	2,4,6,8,9,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	3,5,7,10,17,18	2,4,6,8,9,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	3,5,7,10,16	2,4,6,8,9,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	3,5,7,10,14,18	2,4,6,8,9,13,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	3,5,7,10,14,16,17	2,4,6,8,9,13,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	3,5,7,10,14	2,4,6,8,9,13,15	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	3,5,7,10,14,16,17,18	2,4,6,8,9,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,5,7,10,12	2,4,6,8,9	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	3,5,7,10,12,16,17,18	2,4,6,8,9,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	3,5,7,10,12,18	2,4,6,8,9,15,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	3,5,7,10,12,16,17	2,4,6,8,9,15,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	3,5,7,10,12,14,17,18	2,4,6,8,9,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	3,5,7,10,12,14,16	2,4,6,8,9	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	3,5,7,10,12,14,17	2,4,6,8,9,15,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	3,5,7,10,12,14,16,18	2,4,6,8,9,15,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	3,5,7,10,12,18	2,4,6,8,9,13,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	3,5,7,10,12,16,17	2,4,6,8,9,13,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	3,5,7,10,12	2,4,6,8,9,13,15	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	3,5,7,10,12,16,17,18	2,4,6,8,9,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	3,5,7,10,12,14,17	2,4,6,8,9,13,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	3,5,7,10,12,14,16,18	2,4,6,8,9,13,18	$2^{-6.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	3,5,7,10,12,14,17,18	2,4,6,8,9,13,15,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	3,5,7,10,12,14,16	2,4,6,8,9,13,15	$2^{-6.5}$

Table 0.1024 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	3,5,7,10,17	2,4,6,8,9,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	3,5,7,10,16,18	2,4,6,8,9,11,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	3,5,7,10,17,18	2,4,6,8,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	3,5,7,10,16	2,4,6,8,9,11,15	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	3,5,7,10,14,18	2,4,6,8,9,11,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	3,5,7,10,14,16,17	2,4,6,8,9,11,17	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	3,5,7,10,14	2,4,6,8,9,11,15	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	3,5,7,10,14,16,17,18	2,4,6,8,9,11,15,17,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	3,5,7,10,17,18	2,4,6,8,9,11,13,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	3,5,7,10,16	2,4,6,8,9,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	3,5,7,10,17	2,4,6,8,9,11,13,15,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	3,5,7,10,16,18	2,4,6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	3,5,7,10,14	2,4,6,8,9,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	3,5,7,10,14,16,17,18	2,4,6,8,9,11,13,17,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	3,5,7,10,14,18	2,4,6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	3,5,7,10,14,16,17	2,4,6,8,9,11,13,15,17	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	3,5,7,10,12,18	2,4,6,8,9,11,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	3,5,7,10,12,16,17	2,4,6,8,9,11,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	3,5,7,10,12	2,4,6,8,9,11,15	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	3,5,7,10,12,16,17,18	2,4,6,8,9,11,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	3,5,7,10,12,14,17	2,4,6,8,9,11,17	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	3,5,7,10,12,14,16,18	2,4,6,8,9,11,18	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	3,5,7,10,12,14,17,18	2,4,6,8,9,11,15,17,18	$2^{-28.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	3,5,7,10,12,14,16	2,4,6,8,9,11,15	2^{-12}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	3,5,7,10,12	2,4,6,8,9,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	3,5,7,10,12,16,17,18	2,4,6,8,9,11,13,17,18	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	3,5,7,10,12,18	2,4,6,8,9,11,13,15,18	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	3,5,7,10,12,16,17	2,4,6,8,9,11,13,15,17	2^{-23}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	3,5,7,10,12,14,17,18	2,4,6,8,9,11,13,17,18	2^{-34}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,7,10,12,14,16	2,4,6,8,9,11,13	$2^{-17.5}$
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	3,5,7,10,12,14,17	2,4,6,8,9,11,13,15,17	2^{-34}
$(0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	3,5,7,10,12,14,16,18	2,4,6,8,9,11,13,15,18	$2^{-17.5}$

Table 0.1025 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,18	18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,16,17	17	2^{-34}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1	15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,16,17,18	15,17,18	2^{-34}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,14,17	17	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,14,16,18	18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,14,17,18	15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,14,16	15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1	13	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,16,17,18	13,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,18	13,15,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,16,17	13,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,14,17,18	13,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,14,16	13	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,14,17	13,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,14,16,18	13,15,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,12,17	17	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,12,16,18	18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,12,17,18	15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,12,16	15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,12,14,18	18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,12,14,16,17	17	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,12,14	15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,12,14,16,17,18	15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,12,17,18	13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,12,16	13	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,12,17	13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,12,16,18	13,15,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,12,14	13	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,12,14,16,17,18	13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,12,14,18	13,15,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,12,14,16,17	13,15,17	$2^{-17.5}$

Table 0.1026 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1	11	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,16,17,18	11,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,18	11,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,16,17	11,15,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,14,17,18	11,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,14,16	11	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,14,17	11,15,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,14,16,18	11,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,18	11,13,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,16,17	11,13,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1	11,13,15	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,16,17,18	11,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,14,17	11,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,14,16,18	11,13,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,14,17,18	11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,14,16	11,13,15	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,12,17,18	11,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,12,16	11	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,12,17	11,15,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,12,16,18	11,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,12,14	11	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,12,14,16,17,18	11,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,12,14,18	11,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,12,14,16,17	11,15,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,12,17	11,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,12,16,18	11,13,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,12,17,18	11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,12,16	11,13,15	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,12,14,18	11,13,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,12,14,16,17	11,13,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,12,14	11,13,15	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,12,14,16,17,18	11,13,15,17,18	$2^{-28.5}$

Table 0.1027 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,10,17	17	2^{-1}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,10,16,18	18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,10,17,18	15,17,18	2^{-1}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,10,16	15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,10,14,18	18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,10,14,16,17	17	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,10,14	15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,10,14,16,17,18	15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,10,17,18	13,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,10,16	13	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,10,17	13,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,10,16,18	13,15,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,10,14	13	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,10,14,16,17,18	13,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,10,14,18	13,15,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,10,14,16,17	13,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,10,12,18	18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,10,12,16,17	17	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,10,12	15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,10,12,16,17,18	15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,10,12,14,17	17	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,10,12,14,16,18	18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,10,12,14,17,18	15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,10,12,14,16	15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,10,12	13	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,10,12,16,17,18	13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,10,12,18	13,15,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,10,12,16,17	13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,10,12,14,17,18	13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,10,12,14,16	13	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,10,12,14,17	13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,10,12,14,16,18	13,15,18	2^{-23}

Table 0.1028 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,10,17,18	11,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,10,16	11	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,10,17	11,15,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,10,16,18	11,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,10,14	11	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,10,14,16,17,18	11,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,10,14,18	11,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,10,14,16,17	11,15,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,10,17	11,13,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,10,16,18	11,13,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,10,17,18	11,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,10,16	11,13,15	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,10,14,18	11,13,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,10,14,16,17	11,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,10,14	11,13,15	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,10,14,16,17,18	11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,10,12	11	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,10,12,16,17,18	11,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,10,12,18	11,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,10,12,16,17	11,15,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,10,12,14,17,18	11,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,10,12,14,16	11	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,10,12,14,17	11,15,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,10,12,14,16,18	11,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,10,12,18	11,13,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,10,12,16,17	11,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,10,12	11,13,15	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,10,12,16,17,18	11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,10,12,14,17	11,13,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,10,12,14,16,18	11,13,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,10,12,14,17,18	11,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,10,12,14,16	11,13,15	2^{-12}

Table 0.1029 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1	9	2^{-1}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,16,17,18	9,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,18	9,15,18	2^{-1}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,16,17	9,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,14,17,18	9,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,14,16	9	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,14,17	9,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,14,16,18	9,15,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,18	9,13,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,16,17	9,13,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1	9,13,15	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,16,17,18	9,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,14,17	9,13,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,14,16,18	9,13,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,14,17,18	9,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,14,16	9,13,15	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,12,17,18	9,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,12,16	9	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,12,17	9,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,12,16,18	9,15,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,12,14	9	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,12,14,16,17,18	9,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,12,14,18	9,15,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,12,14,16,17	9,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,12,17	9,13,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,12,16,18	9,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,12,17,18	9,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,12,16	9,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,12,14,18	9,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,12,14,16,17	9,13,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,12,14	9,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,12,14,16,17,18	9,13,15,17,18	2^{-23}

Table 0.1030 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,18	9,11,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,16,17	9,11,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1	9,11,15	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,16,17,18	9,11,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,14,17	9,11,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,14,16,18	9,11,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,14,17,18	9,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,14,16	9,11,15	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1	9,11,13	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,16,17,18	9,11,13,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,18	9,11,13,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,16,17	9,11,13,15,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,14,17,18	9,11,13,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,14,16	9,11,13	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,14,17	9,11,13,15,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,14,16,18	9,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,12,17	9,11,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,12,16,18	9,11,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,12,17,18	9,11,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,12,16	9,11,15	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,12,14,18	9,11,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,12,14,16,17	9,11,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,12,14	9,11,15	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,12,14,16,17,18	9,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,12,17,18	9,11,13,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,12,16	9,11,13	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,12,17	9,11,13,15,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,12,16,18	9,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,12,14	9,11,13	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,12,14,16,17,18	9,11,13,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,12,14,18	9,11,13,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,12,14,16,17	9,11,13,15,17	2^{-12}

Table 0.1031 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,10,17,18	9,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,10,16	9	2^{-34}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,10,17	9,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,10,16,18	9,15,18	2^{-34}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,10,14	9	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,10,14,16,17,18	9,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,10,14,18	9,15,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,10,14,16,17	9,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,10,17	9,13,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,10,16,18	9,13,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,10,17,18	9,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,10,16	9,13,15	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,10,14,18	9,13,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,10,14,16,17	9,13,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,10,14	9,13,15	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,10,14,16,17,18	9,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,10,12	9	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,10,12,16,17,18	9,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,10,12,18	9,15,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,10,12,16,17	9,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,10,12,14,17,18	9,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,10,12,14,16	9	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,10,12,14,17	9,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,10,12,14,16,18	9,15,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,10,12,18	9,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,10,12,16,17	9,13,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,10,12	9,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,10,12,16,17,18	9,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,10,12,14,17	9,13,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,10,12,14,16,18	9,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,10,12,14,17,18	9,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,10,12,14,16	9,13,15	$2^{-17.5}$

Table 0.1032 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,10,17	9,11,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,10,16,18	9,11,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,10,17,18	9,11,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,10,16	9,11,15	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,10,14,18	9,11,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,10,14,16,17	9,11,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,10,14	9,11,15	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,10,14,16,17,18	9,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,10,17,18	9,11,13,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,10,16	9,11,13	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,10,17	9,11,13,15,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,10,16,18	9,11,13,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,10,14	9,11,13	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,10,14,16,17,18	9,11,13,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,10,14,18	9,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,10,14,16,17	9,11,13,15,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,10,12,18	9,11,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,10,12,16,17	9,11,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,10,12	9,11,15	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,10,12,16,17,18	9,11,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,10,12,14,17	9,11,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,10,12,14,16,18	9,11,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,10,12,14,17,18	9,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,10,12,14,16	9,11,15	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,10,12	9,11,13	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,10,12,16,17,18	9,11,13,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,10,12,18	9,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,10,12,16,17	9,11,13,15,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,10,12,14,17,18	9,11,13,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,10,12,14,16	9,11,13	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,10,12,14,17	9,11,13,15,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,10,12,14,16,18	9,11,13,15,18	$2^{-28.5}$

Table 0.1033 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,17	8,17	2^{-34}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,16,18	8,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,17,18	8,15,17,18	2^{-34}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,16	8,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,14,18	8,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,14,16,17	8,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,14	8,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,14,16,17,18	8,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,17,18	8,13,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,16	8,13	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,17	8,13,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,16,18	8,13,15,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,14	8,13	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,14,16,17,18	8,13,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,14,18	8,13,15,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,14,16,17	8,13,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,12,18	8,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,12,16,17	8,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,12	8,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,12,16,17,18	8,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,12,14,17	8,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,12,14,16,18	8,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,12,14,17,18	8,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,12,14,16	8,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,12	8,13	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,12,16,17,18	8,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,12,18	8,13,15,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,12,16,17	8,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,12,14,17,18	8,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,12,14,16	8,13	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,12,14,17	8,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,12,14,16,18	8,13,15,18	2^{-12}

Table 0.1034 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,17,18	8,11,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,16	8,11	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,17	8,11,15,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,16,18	8,11,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,14	8,11	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,14,16,17,18	8,11,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,14,18	8,11,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,14,16,17	8,11,15,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,17	8,11,13,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,16,18	8,11,13,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,17,18	8,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,16	8,11,13,15	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,14,18	8,11,13,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,14,16,17	8,11,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,14	8,11,13,15	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,14,16,17,18	8,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,12	8,11	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,12,16,17,18	8,11,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,12,18	8,11,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,12,16,17	8,11,15,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,12,14,17,18	8,11,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,12,14,16	8,11	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,12,14,17	8,11,15,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,12,14,16,18	8,11,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,12,18	8,11,13,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,12,16,17	8,11,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,12	8,11,13,15	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,12,16,17,18	8,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,12,14,17	8,11,13,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,12,14,16,18	8,11,13,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,12,14,17,18	8,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,12,14,16	8,11,13,15	2^{-23}

Table 0.1035 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,10,18	8,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,10,16,17	8,17	2^{-1}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,10	8,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,10,16,17,18	8,15,17,18	2^{-1}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,10,14,17	8,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,10,14,16,18	8,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,10,14,17,18	8,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,10,14,16	8,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,10	8,13	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,10,16,17,18	8,13,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,10,18	8,13,15,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,10,16,17	8,13,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,10,14,17,18	8,13,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,10,14,16	8,13	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,10,14,17	8,13,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,10,14,16,18	8,13,15,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,10,12,17	8,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,10,12,16,18	8,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,10,12,17,18	8,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,10,12,16	8,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,10,12,14,18	8,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,10,12,14,16,17	8,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,10,12,14	8,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,10,12,14,16,17,18	8,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,10,12,17,18	8,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,10,12,16	8,13	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,10,12,17	8,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,10,12,16,18	8,13,15,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,10,12,14	8,13	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,10,12,14,16,17,18	8,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,10,12,14,18	8,13,15,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,10,12,14,16,17	8,13,15,17	$2^{-17.5}$

Table 0.1036 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,10	8,11	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,10,16,17,18	8,11,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,10,18	8,11,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,10,16,17	8,11,15,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,10,14,17,18	8,11,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,10,14,16	8,11	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,10,14,17	8,11,15,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,10,14,16,18	8,11,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,10,18	8,11,13,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,10,16,17	8,11,13,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,10	8,11,13,15	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,10,16,17,18	8,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,10,14,17	8,11,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,10,14,16,18	8,11,13,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,10,14,17,18	8,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,10,14,16	8,11,13,15	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,10,12,17,18	8,11,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,10,12,16	8,11	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,10,12,17	8,11,15,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,10,12,16,18	8,11,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,10,12,14	8,11	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,10,12,14,16,17,18	8,11,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,10,12,14,18	8,11,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,10,12,14,16,17	8,11,15,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,10,12,17	8,11,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,10,12,16,18	8,11,13,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,10,12,17,18	8,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,10,12,16	8,11,13,15	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,10,12,14,18	8,11,13,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,10,12,14,16,17	8,11,13,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,10,12,14	8,11,13,15	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,10,12,14,16,17,18	8,11,13,15,17,18	$2^{-6.5}$

Table 0.1037 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,17,18	8,9,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,16	8,9	2^{-1}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,17	8,9,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,16,18	8,9,15,18	2^{-1}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,14	8,9	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,14,16,17,18	8,9,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,14,18	8,9,15,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,14,16,17	8,9,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,17	8,9,13,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,16,18	8,9,13,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,17,18	8,9,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,16	8,9,13,15	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,14,18	8,9,13,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,14,16,17	8,9,13,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,14	8,9,13,15	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,14,16,17,18	8,9,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,12	8,9	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,12,16,17,18	8,9,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,12,18	8,9,15,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,12,16,17	8,9,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,12,14,17,18	8,9,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,12,14,16	8,9	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,12,14,17	8,9,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,12,14,16,18	8,9,15,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,12,18	8,9,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,12,16,17	8,9,13,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,12	8,9,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,12,16,17,18	8,9,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,12,14,17	8,9,13,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,12,14,16,18	8,9,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,12,14,17,18	8,9,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,12,14,16	8,9,13,15	$2^{-17.5}$

Table 0.1038 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,17	8,9,11,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,16,18	8,9,11,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,17,18	8,9,11,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,16	8,9,11,15	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,14,18	8,9,11,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,14,16,17	8,9,11,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,14	8,9,11,15	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,14,16,17,18	8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,17,18	8,9,11,13,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,16	8,9,11,13	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,17	8,9,11,13,15,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,16,18	8,9,11,13,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,14	8,9,11,13	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,14,16,17,18	8,9,11,13,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,14,18	8,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,14,16,17	8,9,11,13,15,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,12,18	8,9,11,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,12,16,17	8,9,11,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,12	8,9,11,15	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,12,16,17,18	8,9,11,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,12,14,17	8,9,11,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,12,14,16,18	8,9,11,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,12,14,17,18	8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,12,14,16	8,9,11,15	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,12	8,9,11,13	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,12,16,17,18	8,9,11,13,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,12,18	8,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,12,16,17	8,9,11,13,15,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,12,14,17,18	8,9,11,13,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,12,14,16	8,9,11,13	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,12,14,17	8,9,11,13,15,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,12,14,16,18	8,9,11,13,15,18	$2^{-6.5}$

Table 0.1039 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,10	8,9	2^{-34}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,10,16,17,18	8,9,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,10,18	8,9,15,18	2^{-34}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,10,16,17	8,9,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,10,14,17,18	8,9,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,10,14,16	8,9	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,10,14,17	8,9,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,10,14,16,18	8,9,15,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,10,18	8,9,13,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,10,16,17	8,9,13,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,10	8,9,13,15	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,10,16,17,18	8,9,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,10,14,17	8,9,13,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,10,14,16,18	8,9,13,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,10,14,17,18	8,9,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,10,14,16	8,9,13,15	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,10,12,17,18	8,9,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,10,12,16	8,9	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,10,12,17	8,9,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,10,12,16,18	8,9,15,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,10,12,14	8,9	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,10,12,14,16,17,18	8,9,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,10,12,14,18	8,9,15,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,10,12,14,16,17	8,9,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,10,12,17	8,9,13,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,10,12,16,18	8,9,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,10,12,17,18	8,9,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,10,12,16	8,9,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,10,12,14,18	8,9,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,10,12,14,16,17	8,9,13,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,10,12,14	8,9,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,10,12,14,16,17,18	8,9,13,15,17,18	2^{-12}

Table 0.1040 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,10,18	8,9,11,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,10,16,17	8,9,11,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,10	8,9,11,15	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,10,16,17,18	8,9,11,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,10,14,17	8,9,11,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,10,14,16,18	8,9,11,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,10,14,17,18	8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,10,14,16	8,9,11,15	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,10	8,9,11,13	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,10,16,17,18	8,9,11,13,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,10,18	8,9,11,13,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,10,16,17	8,9,11,13,15,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,10,14,17,18	8,9,11,13,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,10,14,16	8,9,11,13	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,10,14,17	8,9,11,13,15,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,10,14,16,18	8,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,10,12,17	8,9,11,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,10,12,16,18	8,9,11,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,10,12,17,18	8,9,11,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,10,12,16	8,9,11,15	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,10,12,14,18	8,9,11,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,10,12,14,16,17	8,9,11,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,10,12,14	8,9,11,15	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,10,12,14,16,17,18	8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,10,12,17,18	8,9,11,13,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,10,12,16	8,9,11,13	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,10,12,17	8,9,11,13,15,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,10,12,16,18	8,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,10,12,14	8,9,11,13	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,10,12,14,16,17,18	8,9,11,13,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,10,12,14,18	8,9,11,13,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,10,12,14,16,17	8,9,11,13,15,17	2^{-23}

Table 0.1041 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,7	—	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,7,16,17,18	17,18	2^{-34}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,7,18	15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,7,16,17	15,17	2^{-34}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,7,14,17,18	17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,7,14,16	—	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,7,14,17	15,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,7,14,16,18	15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,7,18	13,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,7,16,17	13,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,7	13,15	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,7,16,17,18	13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,7,14,17	13,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,7,14,16,18	13,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,7,14,17,18	13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,7,14,16	13,15	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,7,12,17,18	17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,7,12,16	—	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,7,12,17	15,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,7,12,16,18	15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,7,12,14	—	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,7,12,14,16,17,18	17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,7,12,14,18	15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,7,12,14,16,17	15,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,7,12,17	13,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,7,12,16,18	13,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,7,12,17,18	13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,7,12,16	13,15	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,7,12,14,18	13,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,7,12,14,16,17	13,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,7,12,14	13,15	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,7,12,14,16,17,18	13,15,17,18	$2^{-17.5}$

Table 0.1042 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,7,18	11,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,7,16,17	11,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,7	11,15	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,7,16,17,18	11,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,7,14,17	11,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,7,14,16,18	11,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,7,14,17,18	11,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,7,14,16	11,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,7	11,13	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,7,16,17,18	11,13,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,7,18	11,13,15,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,7,16,17	11,13,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,7,14,17,18	11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,7,14,16	11,13	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,7,14,17	11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,7,14,16,18	11,13,15,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,7,12,17	11,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,7,12,16,18	11,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,7,12,17,18	11,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,7,12,16	11,15	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,7,12,14,18	11,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,7,12,14,16,17	11,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,7,12,14	11,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,7,12,14,16,17,18	11,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,7,12,17,18	11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,7,12,16	11,13	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,7,12,17	11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,7,12,16,18	11,13,15,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,7,12,14	11,13	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,7,12,14,16,17,18	11,13,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,7,12,14,18	11,13,15,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,7,12,14,16,17	11,13,15,17	$2^{-28.5}$

Table 0.1043 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,7,10,17,18	17,18	2^{-1}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,7,10,16	—	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,7,10,17	15,17	2^{-1}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,7,10,16,18	15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,7,10,14	—	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,7,10,14,16,17,18	17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,7,10,14,18	15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,7,10,14,16,17	15,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,7,10,17	13,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,7,10,16,18	13,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,7,10,17,18	13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,7,10,16	13,15	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,7,10,14,18	13,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,7,10,14,16,17	13,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,7,10,14	13,15	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,7,10,14,16,17,18	13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,7,10,12	—	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,7,10,12,16,17,18	17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,7,10,12,18	15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,7,10,12,16,17	15,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,7,10,12,14,17,18	17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,7,10,12,14,16	—	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,7,10,12,14,17	15,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,7,10,12,14,16,18	15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,7,10,12,18	13,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,7,10,12,16,17	13,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,7,10,12	13,15	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,7,10,12,16,17,18	13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,7,10,12,14,17	13,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,7,10,12,14,16,18	13,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,7,10,12,14,17,18	13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,7,10,12,14,16	13,15	2^{-23}

Table 0.1044 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,7,10,17	11,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,7,10,16,18	11,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,7,10,17,18	11,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,7,10,16	11,15	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,7,10,14,18	11,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,7,10,14,16,17	11,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,7,10,14	11,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,7,10,14,16,17,18	11,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,7,10,17,18	11,13,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,7,10,16	11,13	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,7,10,17	11,13,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,7,10,16,18	11,13,15,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,7,10,14	11,13	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,7,10,14,16,17,18	11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,7,10,14,18	11,13,15,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,7,10,14,16,17	11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,7,10,12,18	11,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,7,10,12,16,17	11,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,7,10,12	11,15	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,7,10,12,16,17,18	11,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,7,10,12,14,17	11,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,7,10,12,14,16,18	11,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,7,10,12,14,17,18	11,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,7,10,12,14,16	11,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,7,10,12	11,13	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,7,10,12,16,17,18	11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,7,10,12,18	11,13,15,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,7,10,12,16,17	11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,7,10,12,14,17,18	11,13,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,7,10,12,14,16	11,13	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,7,10,12,14,17	11,13,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,7,10,12,14,16,18	11,13,15,18	2^{-12}

Table 0.1045 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,7,18	9,18	2^{-1}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,7,16,17	9,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,7	9,15	2^{-1}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,7,16,17,18	9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,7,14,17	9,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,7,14,16,18	9,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,7,14,17,18	9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,7,14,16	9,15	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,7	9,13	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,7,16,17,18	9,13,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,7,18	9,13,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,7,16,17	9,13,15,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,7,14,17,18	9,13,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,7,14,16	9,13	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,7,14,17	9,13,15,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,7,14,16,18	9,13,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,7,12,17	9,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,7,12,16,18	9,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,7,12,17,18	9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,7,12,16	9,15	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,7,12,14,18	9,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,7,12,14,16,17	9,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,7,12,14	9,15	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,7,12,14,16,17,18	9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,7,12,17,18	9,13,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,7,12,16	9,13	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,7,12,17	9,13,15,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,7,12,16,18	9,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,7,12,14	9,13	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,7,12,14,16,17,18	9,13,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,7,12,14,18	9,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,7,12,14,16,17	9,13,15,17	2^{-23}

Table 0.1046 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,7	9,11	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,7,16,17,18	9,11,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,7,18	9,11,15,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,7,16,17	9,11,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,7,14,17,18	9,11,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,7,14,16	9,11	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,7,14,17	9,11,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,7,14,16,18	9,11,15,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,7,18	9,11,13,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,7,16,17	9,11,13,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,7	9,11,13,15	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,7,16,17,18	9,11,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,7,14,17	9,11,13,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,7,14,16,18	9,11,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,7,14,17,18	9,11,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,7,14,16	9,11,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,7,12,17,18	9,11,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,7,12,16	9,11	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,7,12,17	9,11,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,7,12,16,18	9,11,15,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,7,12,14	9,11	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,7,12,14,16,17,18	9,11,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,7,12,14,18	9,11,15,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,7,12,14,16,17	9,11,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,7,12,17	9,11,13,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,7,12,16,18	9,11,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,7,12,17,18	9,11,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,7,12,16	9,11,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,7,12,14,18	9,11,13,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,7,12,14,16,17	9,11,13,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,7,12,14	9,11,13,15	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,7,12,14,16,17,18	9,11,13,15,17,18	2^{-12}

Table 0.1047 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,7,10,17	9,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,7,10,16,18	9,18	2^{-34}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,7,10,17,18	9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,7,10,16	9,15	2^{-34}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,7,10,14,18	9,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,7,10,14,16,17	9,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,7,10,14	9,15	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,7,10,14,16,17,18	9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,7,10,17,18	9,13,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,7,10,16	9,13	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,7,10,17	9,13,15,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,7,10,16,18	9,13,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,7,10,14	9,13	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,7,10,14,16,17,18	9,13,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,7,10,14,18	9,13,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,7,10,14,16,17	9,13,15,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,7,10,12,18	9,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,7,10,12,16,17	9,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,7,10,12	9,15	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,7,10,12,16,17,18	9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,7,10,12,14,17	9,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,7,10,12,14,16,18	9,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,7,10,12,14,17,18	9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,7,10,12,14,16	9,15	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,7,10,12	9,13	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,7,10,12,16,17,18	9,13,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,7,10,12,18	9,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,7,10,12,16,17	9,13,15,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,7,10,12,14,17,18	9,13,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,7,10,12,14,16	9,13	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,7,10,12,14,17	9,13,15,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,7,10,12,14,16,18	9,13,15,18	$2^{-17.5}$

Table 0.1048 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,7,10,17,18	9,11,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,7,10,16	9,11	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,7,10,17	9,11,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,7,10,16,18	9,11,15,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,7,10,14	9,11	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,7,10,14,16,17,18	9,11,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,7,10,14,18	9,11,15,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,7,10,14,16,17	9,11,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,7,10,17	9,11,13,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,7,10,16,18	9,11,13,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,7,10,17,18	9,11,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,7,10,16	9,11,13,15	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,7,10,14,18	9,11,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,7,10,14,16,17	9,11,13,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,7,10,14	9,11,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,7,10,14,16,17,18	9,11,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,7,10,12	9,11	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,7,10,12,16,17,18	9,11,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,7,10,12,18	9,11,15,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,7,10,12,16,17	9,11,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,7,10,12,14,17,18	9,11,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,7,10,12,14,16	9,11	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,7,10,12,14,17	9,11,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,7,10,12,14,16,18	9,11,15,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,7,10,12,18	9,11,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,7,10,12,16,17	9,11,13,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,7,10,12	9,11,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,7,10,12,16,17,18	9,11,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,7,10,12,14,17	9,11,13,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,7,10,12,14,16,18	9,11,13,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,7,10,12,14,17,18	9,11,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,7,10,12,14,16	9,11,13,15	$2^{-28.5}$

Table 0.1049 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,7,17,18	8,17,18	2^{-34}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,7,16	8	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,7,17	8,15,17	2^{-34}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,7,16,18	8,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,7,14	8	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,7,14,16,17,18	8,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,7,14,18	8,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,7,14,16,17	8,15,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,7,17	8,13,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,7,16,18	8,13,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,7,17,18	8,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,7,16	8,13,15	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,7,14,18	8,13,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,7,14,16,17	8,13,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,7,14	8,13,15	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,7,14,16,17,18	8,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,7,12	8	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,7,12,16,17,18	8,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,7,12,18	8,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,7,12,16,17	8,15,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,7,12,14,17,18	8,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,7,12,14,16	8	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,7,12,14,17	8,15,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,7,12,14,16,18	8,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,7,12,18	8,13,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,7,12,16,17	8,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,7,12	8,13,15	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,7,12,16,17,18	8,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,7,12,14,17	8,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,7,12,14,16,18	8,13,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,7,12,14,17,18	8,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,7,12,14,16	8,13,15	2^{-12}

Table 0.1050 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,7,17	8,11,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,7,16,18	8,11,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,7,17,18	8,11,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,7,16	8,11,15	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,7,14,18	8,11,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,7,14,16,17	8,11,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,7,14	8,11,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,7,14,16,17,18	8,11,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,7,17,18	8,11,13,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,7,16	8,11,13	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,7,17	8,11,13,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,7,16,18	8,11,13,15,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,7,14	8,11,13	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,7,14,16,17,18	8,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,7,14,18	8,11,13,15,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,7,14,16,17	8,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,7,12,18	8,11,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,7,12,16,17	8,11,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,7,12	8,11,15	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,7,12,16,17,18	8,11,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,7,12,14,17	8,11,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,7,12,14,16,18	8,11,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,7,12,14,17,18	8,11,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,7,12,14,16	8,11,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,7,12	8,11,13	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,7,12,16,17,18	8,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,7,12,18	8,11,13,15,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,7,12,16,17	8,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,7,12,14,17,18	8,11,13,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,7,12,14,16	8,11,13	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,7,12,14,17	8,11,13,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,7,12,14,16,18	8,11,13,15,18	2^{-23}

Table 0.1051 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,7,10	8	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,7,10,16,17,18	8,17,18	2^{-1}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,7,10,18	8,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,7,10,16,17	8,15,17	2^{-1}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,7,10,14,17,18	8,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,7,10,14,16	8	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,7,10,14,17	8,15,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,7,10,14,16,18	8,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,7,10,18	8,13,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,7,10,16,17	8,13,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,7,10	8,13,15	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,7,10,16,17,18	8,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,7,10,14,17	8,13,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,7,10,14,16,18	8,13,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,7,10,14,17,18	8,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,7,10,14,16	8,13,15	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,7,10,12,17,18	8,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,7,10,12,16	8	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,7,10,12,17	8,15,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,7,10,12,16,18	8,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,7,10,12,14	8	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,7,10,12,14,16,17,18	8,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,7,10,12,14,18	8,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,7,10,12,14,16,17	8,15,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,7,10,12,17	8,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,7,10,12,16,18	8,13,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,7,10,12,17,18	8,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,7,10,12,16	8,13,15	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,7,10,12,14,18	8,13,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,7,10,12,14,16,17	8,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,7,10,12,14	8,13,15	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,7,10,12,14,16,17,18	8,13,15,17,18	$2^{-17.5}$

Table 0.1052 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,7,10,18	8,11,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,7,10,16,17	8,11,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,7,10	8,11,15	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,7,10,16,17,18	8,11,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,7,10,14,17	8,11,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,7,10,14,16,18	8,11,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,7,10,14,17,18	8,11,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,7,10,14,16	8,11,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,7,10	8,11,13	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,7,10,16,17,18	8,11,13,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,7,10,18	8,11,13,15,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,7,10,16,17	8,11,13,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,7,10,14,17,18	8,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,7,10,14,16	8,11,13	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,7,10,14,17	8,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,7,10,14,16,18	8,11,13,15,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,7,10,12,17	8,11,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,7,10,12,16,18	8,11,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,7,10,12,17,18	8,11,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,7,10,12,16	8,11,15	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,7,10,12,14,18	8,11,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,7,10,12,14,16,17	8,11,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,7,10,12,14	8,11,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,7,10,12,14,16,17,18	8,11,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,7,10,12,17,18	8,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,7,10,12,16	8,11,13	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,7,10,12,17	8,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,7,10,12,16,18	8,11,13,15,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,7,10,12,14	8,11,13	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,7,10,12,14,16,17,18	8,11,13,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,7,10,12,14,18	8,11,13,15,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,7,10,12,14,16,17	8,11,13,15,17	$2^{-6.5}$

Table 0.1053 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,7,17	8,9,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,7,16,18	8,9,18	2^{-1}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,7,17,18	8,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,7,16	8,9,15	2^{-1}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,7,14,18	8,9,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,7,14,16,17	8,9,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,7,14	8,9,15	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,7,14,16,17,18	8,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,7,17,18	8,9,13,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,7,16	8,9,13	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,7,17	8,9,13,15,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,7,16,18	8,9,13,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,7,14	8,9,13	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,7,14,16,17,18	8,9,13,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,7,14,18	8,9,13,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,7,14,16,17	8,9,13,15,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,7,12,18	8,9,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,7,12,16,17	8,9,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,7,12	8,9,15	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,7,12,16,17,18	8,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,7,12,14,17	8,9,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,7,12,14,16,18	8,9,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,7,12,14,17,18	8,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,7,12,14,16	8,9,15	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,7,12	8,9,13	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,7,12,16,17,18	8,9,13,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,7,12,18	8,9,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,7,12,16,17	8,9,13,15,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,7,12,14,17,18	8,9,13,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,7,12,14,16	8,9,13	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,7,12,14,17	8,9,13,15,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,7,12,14,16,18	8,9,13,15,18	$2^{-17.5}$

Table 0.1054 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,7,17,18	8,9,11,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,7,16	8,9,11	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,7,17	8,9,11,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,7,16,18	8,9,11,15,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,7,14	8,9,11	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,7,14,16,17,18	8,9,11,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,7,14,18	8,9,11,15,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,7,14,16,17	8,9,11,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,7,17	8,9,11,13,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,7,16,18	8,9,11,13,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,7,17,18	8,9,11,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,7,16	8,9,11,13,15	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,7,14,18	8,9,11,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,7,14,16,17	8,9,11,13,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,7,14	8,9,11,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,7,14,16,17,18	8,9,11,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,7,12	8,9,11	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,7,12,16,17,18	8,9,11,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,7,12,18	8,9,11,15,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,7,12,16,17	8,9,11,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,7,12,14,17,18	8,9,11,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,7,12,14,16	8,9,11	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,7,12,14,17	8,9,11,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,7,12,14,16,18	8,9,11,15,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,7,12,18	8,9,11,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,7,12,16,17	8,9,11,13,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,7,12	8,9,11,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,7,12,16,17,18	8,9,11,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,7,12,14,17	8,9,11,13,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,7,12,14,16,18	8,9,11,13,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,7,12,14,17,18	8,9,11,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,7,12,14,16	8,9,11,13,15	$2^{-6.5}$

Table 0.1055 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,7,10,18	8,9,18	2^{-34}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,7,10,16,17	8,9,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,7,10	8,9,15	2^{-34}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,7,10,16,17,18	8,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,7,10,14,17	8,9,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,7,10,14,16,18	8,9,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,7,10,14,17,18	8,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,7,10,14,16	8,9,15	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,7,10	8,9,13	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,7,10,16,17,18	8,9,13,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,7,10,18	8,9,13,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,7,10,16,17	8,9,13,15,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,7,10,14,17,18	8,9,13,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,7,10,14,16	8,9,13	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,7,10,14,17	8,9,13,15,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,7,10,14,16,18	8,9,13,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,7,10,12,17	8,9,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,7,10,12,16,18	8,9,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,7,10,12,17,18	8,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,7,10,12,16	8,9,15	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,7,10,12,14,18	8,9,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,7,10,12,14,16,17	8,9,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,7,10,12,14	8,9,15	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,7,10,12,14,16,17,18	8,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,7,10,12,17,18	8,9,13,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,7,10,12,16	8,9,13	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,7,10,12,17	8,9,13,15,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,7,10,12,16,18	8,9,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,7,10,12,14	8,9,13	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,7,10,12,14,16,17,18	8,9,13,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,7,10,12,14,18	8,9,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,7,10,12,14,16,17	8,9,13,15,17	2^{-12}

Table 0.1056 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,7,10	8,9,11	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,7,10,16,17,18	8,9,11,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,7,10,18	8,9,11,15,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,7,10,16,17	8,9,11,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,7,10,14,17,18	8,9,11,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,7,10,14,16	8,9,11	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,7,10,14,17	8,9,11,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,7,10,14,16,18	8,9,11,15,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,7,10,18	8,9,11,13,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,7,10,16,17	8,9,11,13,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,7,10	8,9,11,13,15	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,7,10,16,17,18	8,9,11,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,7,10,14,17	8,9,11,13,17	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,7,10,14,16,18	8,9,11,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,7,10,14,17,18	8,9,11,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,7,10,14,16	8,9,11,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,7,10,12,17,18	8,9,11,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,7,10,12,16	8,9,11	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,7,10,12,17	8,9,11,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,7,10,12,16,18	8,9,11,15,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,7,10,12,14	8,9,11	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,7,10,12,14,16,17,18	8,9,11,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,7,10,12,14,18	8,9,11,15,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,7,10,12,14,16,17	8,9,11,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,7,10,12,17	8,9,11,13,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,7,10,12,16,18	8,9,11,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,7,10,12,17,18	8,9,11,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,7,10,12,16	8,9,11,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,7,10,12,14,18	8,9,11,13,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,7,10,12,14,16,17	8,9,11,13,17	2^{-23}
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,7,10,12,14	8,9,11,13,15	$2^{-28.5}$
$(1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,7,10,12,14,16,17,18	8,9,11,13,15,17,18	2^{-23}

Table 0.1057 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,17	6,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,16,18	6,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,17,18	6,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,16	6,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,14,18	6,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,14,16,17	6,17	2^{-34}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,14	6,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,14,16,17,18	6,15,17,18	2^{-34}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,17,18	6,13,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,16	6,13	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,17	6,13,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,16,18	6,13,15,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,14	6,13	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,14,16,17,18	6,13,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,14,18	6,13,15,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,14,16,17	6,13,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,12,18	6,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,12,16,17	6,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,12	6,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,12,16,17,18	6,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,12,14,17	6,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,12,14,16,18	6,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,12,14,17,18	6,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,12,14,16	6,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,12	6,13	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,12,16,17,18	6,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,12,18	6,13,15,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,12,16,17	6,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,12,14,17,18	6,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,12,14,16	6,13	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,12,14,17	6,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,12,14,16,18	6,13,15,18	2^{-23}

Table 0.1058 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,17,18	6,11,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,16	6,11	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,17	6,11,15,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,16,18	6,11,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,14	6,11	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,14,16,17,18	6,11,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,14,18	6,11,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,14,16,17	6,11,15,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,17	6,11,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,16,18	6,11,13,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,17,18	6,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,16	6,11,13,15	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,14,18	6,11,13,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,14,16,17	6,11,13,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,14	6,11,13,15	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,14,16,17,18	6,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,12	6,11	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,12,16,17,18	6,11,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,12,18	6,11,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,12,16,17	6,11,15,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,12,14,17,18	6,11,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,12,14,16	6,11	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,12,14,17	6,11,15,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,12,14,16,18	6,11,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,12,18	6,11,13,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,12,16,17	6,11,13,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,12	6,11,13,15	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,12,16,17,18	6,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,12,14,17	6,11,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,12,14,16,18	6,11,13,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,12,14,17,18	6,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,12,14,16	6,11,13,15	2^{-23}

Table 0.1059 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,10,18	6,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,10,16,17	6,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,10	6,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,10,16,17,18	6,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,10,14,17	6,17	2^{-1}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,10,14,16,18	6,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,10,14,17,18	6,15,17,18	2^{-1}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,10,14,16	6,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,10	6,13	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,10,16,17,18	6,13,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,10,18	6,13,15,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,10,16,17	6,13,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,10,14,17,18	6,13,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,10,14,16	6,13	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,10,14,17	6,13,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,10,14,16,18	6,13,15,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,10,12,17	6,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,10,12,16,18	6,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,10,12,17,18	6,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,10,12,16	6,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,10,12,14,18	6,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,10,12,14,16,17	6,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,10,12,14	6,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,10,12,14,16,17,18	6,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,10,12,17,18	6,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,10,12,16	6,13	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,10,12,17	6,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,10,12,16,18	6,13,15,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,10,12,14	6,13	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,10,12,14,16,17,18	6,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,10,12,14,18	6,13,15,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,10,12,14,16,17	6,13,15,17	$2^{-17.5}$

Table 0.1060 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,10	6,11	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,10,16,17,18	6,11,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,10,18	6,11,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,10,16,17	6,11,15,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,10,14,17,18	6,11,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,10,14,16	6,11	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,10,14,17	6,11,15,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,10,14,16,18	6,11,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,10,18	6,11,13,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,10,16,17	6,11,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,10	6,11,13,15	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,10,16,17,18	6,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,10,14,17	6,11,13,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,10,14,16,18	6,11,13,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,10,14,17,18	6,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,10,14,16	6,11,13,15	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,10,12,17,18	6,11,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,10,12,16	6,11	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,10,12,17	6,11,15,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,10,12,16,18	6,11,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,10,12,14	6,11	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,10,12,14,16,17,18	6,11,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,10,12,14,18	6,11,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,10,12,14,16,17	6,11,15,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,10,12,17	6,11,13,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,10,12,16,18	6,11,13,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,10,12,17,18	6,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,10,12,16	6,11,13,15	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,10,12,14,18	6,11,13,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,10,12,14,16,17	6,11,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,10,12,14	6,11,13,15	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,10,12,14,16,17,18	6,11,13,15,17,18	$2^{-17.5}$

Table 0.1061 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,17,18	6,9,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,16	6,9	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,17	6,9,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,16,18	6,9,15,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,14	6,9	2^{-1}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,14,16,17,18	6,9,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,14,18	6,9,15,18	2^{-1}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,14,16,17	6,9,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,17	6,9,13,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,16,18	6,9,13,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,17,18	6,9,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,16	6,9,13,15	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,14,18	6,9,13,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,14,16,17	6,9,13,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,14	6,9,13,15	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,14,16,17,18	6,9,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,12	6,9	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,12,16,17,18	6,9,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,12,18	6,9,15,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,12,16,17	6,9,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,12,14,17,18	6,9,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,12,14,16	6,9	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,12,14,17	6,9,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,12,14,16,18	6,9,15,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,12,18	6,9,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,12,16,17	6,9,13,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,12	6,9,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,12,16,17,18	6,9,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,12,14,17	6,9,13,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,12,14,16,18	6,9,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,12,14,17,18	6,9,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,12,14,16	6,9,13,15	$2^{-17.5}$

Table 0.1062 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,17	6,9,11,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,16,18	6,9,11,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,17,18	6,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,16	6,9,11,15	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,14,18	6,9,11,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,14,16,17	6,9,11,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,14	6,9,11,15	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,14,16,17,18	6,9,11,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,17,18	6,9,11,13,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,16	6,9,11,13	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,17	6,9,11,13,15,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,16,18	6,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,14	6,9,11,13	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,14,16,17,18	6,9,11,13,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,14,18	6,9,11,13,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,14,16,17	6,9,11,13,15,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,12,18	6,9,11,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,12,16,17	6,9,11,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,12	6,9,11,15	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,12,16,17,18	6,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,12,14,17	6,9,11,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,12,14,16,18	6,9,11,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,12,14,17,18	6,9,11,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,12,14,16	6,9,11,15	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,12	6,9,11,13	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,12,16,17,18	6,9,11,13,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,12,18	6,9,11,13,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,12,16,17	6,9,11,13,15,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,12,14,17,18	6,9,11,13,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,12,14,16	6,9,11,13	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,12,14,17	6,9,11,13,15,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,12,14,16,18	6,9,11,13,15,18	$2^{-17.5}$

Table 0.1063 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,10	6,9	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,10,16,17,18	6,9,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,10,18	6,9,15,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,10,16,17	6,9,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,10,14,17,18	6,9,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,10,14,16	6,9	2^{-34}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,10,14,17	6,9,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,10,14,16,18	6,9,15,18	2^{-34}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,10,18	6,9,13,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,10,16,17	6,9,13,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,10	6,9,13,15	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,10,16,17,18	6,9,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,10,14,17	6,9,13,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,10,14,16,18	6,9,13,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,10,14,17,18	6,9,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,10,14,16	6,9,13,15	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,10,12,17,18	6,9,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,10,12,16	6,9	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,10,12,17	6,9,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,10,12,16,18	6,9,15,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,10,12,14	6,9	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,10,12,14,16,17,18	6,9,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,10,12,14,18	6,9,15,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,10,12,14,16,17	6,9,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,10,12,17	6,9,13,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,10,12,16,18	6,9,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,10,12,17,18	6,9,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,10,12,16	6,9,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,10,12,14,18	6,9,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,10,12,14,16,17	6,9,13,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,10,12,14	6,9,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,10,12,14,16,17,18	6,9,13,15,17,18	2^{-23}

Table 0.1064 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,10,18	6,9,11,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,10,16,17	6,9,11,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,10	6,9,11,15	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,10,16,17,18	6,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,10,14,17	6,9,11,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,10,14,16,18	6,9,11,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,10,14,17,18	6,9,11,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,10,14,16	6,9,11,15	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,10	6,9,11,13	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,10,16,17,18	6,9,11,13,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,10,18	6,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,10,16,17	6,9,11,13,15,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,10,14,17,18	6,9,11,13,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,10,14,16	6,9,11,13	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,10,14,17	6,9,11,13,15,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,10,14,16,18	6,9,11,13,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,10,12,17	6,9,11,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,10,12,16,18	6,9,11,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,10,12,17,18	6,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,10,12,16	6,9,11,15	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,10,12,14,18	6,9,11,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,10,12,14,16,17	6,9,11,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,10,12,14	6,9,11,15	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,10,12,14,16,17,18	6,9,11,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,10,12,17,18	6,9,11,13,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,10,12,16	6,9,11,13	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,10,12,17	6,9,11,13,15,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,10,12,16,18	6,9,11,13,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,10,12,14	6,9,11,13	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,10,12,14,16,17,18	6,9,11,13,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,10,12,14,18	6,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,10,12,14,16,17	6,9,11,13,15,17	2^{-23}

Table 0.1065 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,18	6,8,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,16,17	6,8,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1	6,8,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,16,17,18	6,8,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,14,17	6,8,17	2^{-34}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,14,16,18	6,8,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,14,17,18	6,8,15,17,18	2^{-34}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,14,16	6,8,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1	6,8,13	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,16,17,18	6,8,13,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,18	6,8,13,15,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,16,17	6,8,13,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,14,17,18	6,8,13,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,14,16	6,8,13	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,14,17	6,8,13,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,14,16,18	6,8,13,15,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,12,17	6,8,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,12,16,18	6,8,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,12,17,18	6,8,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,12,16	6,8,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,12,14,18	6,8,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,12,14,16,17	6,8,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,12,14	6,8,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,12,14,16,17,18	6,8,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,12,17,18	6,8,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,12,16	6,8,13	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,12,17	6,8,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,12,16,18	6,8,13,15,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,12,14	6,8,13	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,12,14,16,17,18	6,8,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,12,14,18	6,8,13,15,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,12,14,16,17	6,8,13,15,17	$2^{-17.5}$

Table 0.1066 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1	6,8,11	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,16,17,18	6,8,11,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,18	6,8,11,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,16,17	6,8,11,15,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,14,17,18	6,8,11,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,14,16	6,8,11	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,14,17	6,8,11,15,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,14,16,18	6,8,11,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,18	6,8,11,13,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,16,17	6,8,11,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1	6,8,11,13,15	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,16,17,18	6,8,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,14,17	6,8,11,13,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,14,16,18	6,8,11,13,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,14,17,18	6,8,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,14,16	6,8,11,13,15	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,12,17,18	6,8,11,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,12,16	6,8,11	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,12,17	6,8,11,15,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,12,16,18	6,8,11,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,12,14	6,8,11	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,12,14,16,17,18	6,8,11,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,12,14,18	6,8,11,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,12,14,16,17	6,8,11,15,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,12,17	6,8,11,13,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,12,16,18	6,8,11,13,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,12,17,18	6,8,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,12,16	6,8,11,13,15	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,12,14,18	6,8,11,13,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,12,14,16,17	6,8,11,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,12,14	6,8,11,13,15	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,12,14,16,17,18	6,8,11,13,15,17,18	$2^{-17.5}$

Table 0.1067 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(2)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,10,17	6,8,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,10,16,18	6,8,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,10,17,18	6,8,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,10,16	6,8,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,10,14,18	6,8,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,10,14,16,17	6,8,17	2^{-1}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,10,14	6,8,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,10,14,16,17,18	6,8,15,17,18	2^{-1}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,10,17,18	6,8,13,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,10,16	6,8,13	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,10,17	6,8,13,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,10,16,18	6,8,13,15,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,10,14	6,8,13	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,10,14,16,17,18	6,8,13,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,10,14,18	6,8,13,15,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,10,14,16,17	6,8,13,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,10,12,18	6,8,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,10,12,16,17	6,8,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,10,12	6,8,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,10,12,16,17,18	6,8,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,10,12,14,17	6,8,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,10,12,14,16,18	6,8,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,10,12,14,17,18	6,8,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,10,12,14,16	6,8,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,10,12	6,8,13	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,10,12,16,17,18	6,8,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,10,12,18	6,8,13,15,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,10,12,16,17	6,8,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,10,12,14,17,18	6,8,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,10,12,14,16	6,8,13	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,10,12,14,17	6,8,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,10,12,14,16,18	6,8,13,15,18	2^{-12}

Table 0.1068 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,10,17,18	6,8,11,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,10,16	6,8,11	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,10,17	6,8,11,15,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,10,16,18	6,8,11,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,10,14	6,8,11	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,10,14,16,17,18	6,8,11,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,10,14,18	6,8,11,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,10,14,16,17	6,8,11,15,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,10,17	6,8,11,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,10,16,18	6,8,11,13,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,10,17,18	6,8,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,10,16	6,8,11,13,15	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,10,14,18	6,8,11,13,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,10,14,16,17	6,8,11,13,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,10,14	6,8,11,13,15	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,10,14,16,17,18	6,8,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,10,12	6,8,11	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,10,12,16,17,18	6,8,11,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,10,12,18	6,8,11,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,10,12,16,17	6,8,11,15,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,10,12,14,17,18	6,8,11,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,10,12,14,16	6,8,11	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,10,12,14,17	6,8,11,15,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,10,12,14,16,18	6,8,11,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,10,12,18	6,8,11,13,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,10,12,16,17	6,8,11,13,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,10,12	6,8,11,13,15	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,10,12,16,17,18	6,8,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,10,12,14,17	6,8,11,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,10,12,14,16,18	6,8,11,13,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,10,12,14,17,18	6,8,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,10,12,14,16	6,8,11,13,15	2^{-12}

Table 0.1069 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1	6,8,9	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,16,17,18	6,8,9,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,18	6,8,9,15,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,16,17	6,8,9,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,14,17,18	6,8,9,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,14,16	6,8,9	2^{-1}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,14,17	6,8,9,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,14,16,18	6,8,9,15,18	2^{-1}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,18	6,8,9,13,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,16,17	6,8,9,13,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1	6,8,9,13,15	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,16,17,18	6,8,9,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,14,17	6,8,9,13,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,14,16,18	6,8,9,13,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,14,17,18	6,8,9,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,14,16	6,8,9,13,15	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,12,17,18	6,8,9,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,12,16	6,8,9	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,12,17	6,8,9,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,12,16,18	6,8,9,15,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,12,14	6,8,9	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,12,14,16,17,18	6,8,9,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,12,14,18	6,8,9,15,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,12,14,16,17	6,8,9,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,12,17	6,8,9,13,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,12,16,18	6,8,9,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,12,17,18	6,8,9,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,12,16	6,8,9,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,12,14,18	6,8,9,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,12,14,16,17	6,8,9,13,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,12,14	6,8,9,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,12,14,16,17,18	6,8,9,13,15,17,18	2^{-12}

Table 0.1070 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,18	6,8,9,11,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,16,17	6,8,9,11,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1	6,8,9,11,15	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,16,17,18	6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,14,17	6,8,9,11,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,14,16,18	6,8,9,11,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,14,17,18	6,8,9,11,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,14,16	6,8,9,11,15	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1	6,8,9,11,13	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,16,17,18	6,8,9,11,13,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,18	6,8,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,16,17	6,8,9,11,13,15,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,14,17,18	6,8,9,11,13,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,14,16	6,8,9,11,13	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,14,17	6,8,9,11,13,15,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,14,16,18	6,8,9,11,13,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,12,17	6,8,9,11,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,12,16,18	6,8,9,11,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,12,17,18	6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,12,16	6,8,9,11,15	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,12,14,18	6,8,9,11,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,12,14,16,17	6,8,9,11,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,12,14	6,8,9,11,15	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,12,14,16,17,18	6,8,9,11,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,12,17,18	6,8,9,11,13,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,12,16	6,8,9,11,13	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,12,17	6,8,9,11,13,15,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,12,16,18	6,8,9,11,13,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,12,14	6,8,9,11,13	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,12,14,16,17,18	6,8,9,11,13,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,12,14,18	6,8,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,12,14,16,17	6,8,9,11,13,15,17	2^{-12}

Table 0.1071 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,10,17,18	6,8,9,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,10,16	6,8,9	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,10,17	6,8,9,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,10,16,18	6,8,9,15,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,10,14	6,8,9	2^{-34}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,10,14,16,17,18	6,8,9,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,10,14,18	6,8,9,15,18	2^{-34}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,10,14,16,17	6,8,9,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,10,17	6,8,9,13,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,10,16,18	6,8,9,13,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,10,17,18	6,8,9,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,10,16	6,8,9,13,15	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,10,14,18	6,8,9,13,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,10,14,16,17	6,8,9,13,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,10,14	6,8,9,13,15	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,10,14,16,17,18	6,8,9,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,10,12	6,8,9	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,10,12,16,17,18	6,8,9,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,10,12,18	6,8,9,15,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,10,12,16,17	6,8,9,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,10,12,14,17,18	6,8,9,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,10,12,14,16	6,8,9	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,10,12,14,17	6,8,9,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,10,12,14,16,18	6,8,9,15,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,10,12,18	6,8,9,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,10,12,16,17	6,8,9,13,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,10,12	6,8,9,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,10,12,16,17,18	6,8,9,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,10,12,14,17	6,8,9,13,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,10,12,14,16,18	6,8,9,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,10,12,14,17,18	6,8,9,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,10,12,14,16	6,8,9,13,15	$2^{-17.5}$

Table 0.1072 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,10,17	6,8,9,11,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,10,16,18	6,8,9,11,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,10,17,18	6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,10,16	6,8,9,11,15	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,10,14,18	6,8,9,11,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,10,14,16,17	6,8,9,11,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,10,14	6,8,9,11,15	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,10,14,16,17,18	6,8,9,11,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,10,17,18	6,8,9,11,13,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,10,16	6,8,9,11,13	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,10,17	6,8,9,11,13,15,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,10,16,18	6,8,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,10,14	6,8,9,11,13	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,10,14,16,17,18	6,8,9,11,13,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,10,14,18	6,8,9,11,13,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,10,14,16,17	6,8,9,11,13,15,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,10,12,18	6,8,9,11,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,10,12,16,17	6,8,9,11,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,10,12	6,8,9,11,15	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,10,12,16,17,18	6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,10,12,14,17	6,8,9,11,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,10,12,14,16,18	6,8,9,11,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,10,12,14,17,18	6,8,9,11,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,10,12,14,16	6,8,9,11,15	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,10,12	6,8,9,11,13	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,10,12,16,17,18	6,8,9,11,13,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,10,12,18	6,8,9,11,13,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,10,12,16,17	6,8,9,11,13,15,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,10,12,14,17,18	6,8,9,11,13,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,10,12,14,16	6,8,9,11,13	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,10,12,14,17	6,8,9,11,13,15,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,10,12,14,16,18	6,8,9,11,13,15,18	$2^{-17.5}$

Table 0.1073 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,7,17,18	6,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,7,16	6	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,7,17	6,15,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,7,16,18	6,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,7,14	6	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,7,14,16,17,18	6,17,18	2^{-34}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,7,14,18	6,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,7,14,16,17	6,15,17	2^{-34}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,7,17	6,13,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,7,16,18	6,13,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,7,17,18	6,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,7,16	6,13,15	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,7,14,18	6,13,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,7,14,16,17	6,13,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,7,14	6,13,15	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,7,14,16,17,18	6,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,7,12	6	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,7,12,16,17,18	6,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,7,12,18	6,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,7,12,16,17	6,15,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,7,12,14,17,18	6,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,7,12,14,16	6	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,7,12,14,17	6,15,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,7,12,14,16,18	6,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,7,12,18	6,13,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,7,12,16,17	6,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,7,12	6,13,15	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,7,12,16,17,18	6,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,7,12,14,17	6,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,7,12,14,16,18	6,13,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,7,12,14,17,18	6,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,7,12,14,16	6,13,15	2^{-23}

Table 0.1074 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,7,17	6,11,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,7,16,18	6,11,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,7,17,18	6,11,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,7,16	6,11,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,7,14,18	6,11,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,7,14,16,17	6,11,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,7,14	6,11,15	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,7,14,16,17,18	6,11,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,7,17,18	6,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,7,16	6,11,13	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,7,17	6,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,7,16,18	6,11,13,15,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,7,14	6,11,13	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,7,14,16,17,18	6,11,13,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,7,14,18	6,11,13,15,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,7,14,16,17	6,11,13,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,7,12,18	6,11,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,7,12,16,17	6,11,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,7,12	6,11,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,7,12,16,17,18	6,11,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,7,12,14,17	6,11,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,7,12,14,16,18	6,11,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,7,12,14,17,18	6,11,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,7,12,14,16	6,11,15	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,7,12	6,11,13	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,7,12,16,17,18	6,11,13,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,7,12,18	6,11,13,15,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,7,12,16,17	6,11,13,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,7,12,14,17,18	6,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,7,12,14,16	6,11,13	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,7,12,14,17	6,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,7,12,14,16,18	6,11,13,15,18	2^{-23}

Table 0.1075 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,7,10	6	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,7,10,16,17,18	6,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,7,10,18	6,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,7,10,16,17	6,15,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,7,10,14,17,18	6,17,18	2^{-1}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,7,10,14,16	6	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,7,10,14,17	6,15,17	2^{-1}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,7,10,14,16,18	6,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,7,10,18	6,13,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,7,10,16,17	6,13,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,7,10	6,13,15	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,7,10,16,17,18	6,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,7,10,14,17	6,13,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,7,10,14,16,18	6,13,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,7,10,14,17,18	6,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,7,10,14,16	6,13,15	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,7,10,12,17,18	6,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,7,10,12,16	6	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,7,10,12,17	6,15,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,7,10,12,16,18	6,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,7,10,12,14	6	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,7,10,12,14,16,17,18	6,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,7,10,12,14,18	6,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,7,10,12,14,16,17	6,15,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,7,10,12,17	6,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,7,10,12,16,18	6,13,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,7,10,12,17,18	6,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,7,10,12,16	6,13,15	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,7,10,12,14,18	6,13,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,7,10,12,14,16,17	6,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,7,10,12,14	6,13,15	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,7,10,12,14,16,17,18	6,13,15,17,18	$2^{-17.5}$

Table 0.1076 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,7,10,18	6,11,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,7,10,16,17	6,11,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,7,10	6,11,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,7,10,16,17,18	6,11,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,7,10,14,17	6,11,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,7,10,14,16,18	6,11,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,7,10,14,17,18	6,11,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,7,10,14,16	6,11,15	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,7,10	6,11,13	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,7,10,16,17,18	6,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,7,10,18	6,11,13,15,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,7,10,16,17	6,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,7,10,14,17,18	6,11,13,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,7,10,14,16	6,11,13	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,7,10,14,17	6,11,13,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,7,10,14,16,18	6,11,13,15,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,7,10,12,17	6,11,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,7,10,12,16,18	6,11,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,7,10,12,17,18	6,11,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,7,10,12,16	6,11,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,7,10,12,14,18	6,11,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,7,10,12,14,16,17	6,11,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,7,10,12,14	6,11,15	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,7,10,12,14,16,17,18	6,11,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,7,10,12,17,18	6,11,13,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,7,10,12,16	6,11,13	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,7,10,12,17	6,11,13,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,7,10,12,16,18	6,11,13,15,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,7,10,12,14	6,11,13	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,7,10,12,14,16,17,18	6,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,7,10,12,14,18	6,11,13,15,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,7,10,12,14,16,17	6,11,13,15,17	$2^{-17.5}$

Table 0.1077 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,7,17	6,9,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,7,16,18	6,9,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,7,17,18	6,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,7,16	6,9,15	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,7,14,18	6,9,18	2^{-1}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,7,14,16,17	6,9,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,7,14	6,9,15	2^{-1}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,7,14,16,17,18	6,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,7,17,18	6,9,13,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,7,16	6,9,13	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,7,17	6,9,13,15,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,7,16,18	6,9,13,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,7,14	6,9,13	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,7,14,16,17,18	6,9,13,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,7,14,18	6,9,13,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,7,14,16,17	6,9,13,15,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,7,12,18	6,9,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,7,12,16,17	6,9,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,7,12	6,9,15	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,7,12,16,17,18	6,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,7,12,14,17	6,9,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,7,12,14,16,18	6,9,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,7,12,14,17,18	6,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,7,12,14,16	6,9,15	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,7,12	6,9,13	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,7,12,16,17,18	6,9,13,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,7,12,18	6,9,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,7,12,16,17	6,9,13,15,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,7,12,14,17,18	6,9,13,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,7,12,14,16	6,9,13	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,7,12,14,17	6,9,13,15,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,7,12,14,16,18	6,9,13,15,18	$2^{-17.5}$

Table 0.1078 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,7,17,18	6,9,11,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,7,16	6,9,11	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,7,17	6,9,11,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,7,16,18	6,9,11,15,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,7,14	6,9,11	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,7,14,16,17,18	6,9,11,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,7,14,18	6,9,11,15,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,7,14,16,17	6,9,11,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,7,17	6,9,11,13,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,7,16,18	6,9,11,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,7,17,18	6,9,11,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,7,16	6,9,11,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,7,14,18	6,9,11,13,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,7,14,16,17	6,9,11,13,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,7,14	6,9,11,13,15	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,7,14,16,17,18	6,9,11,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,7,12	6,9,11	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,7,12,16,17,18	6,9,11,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,7,12,18	6,9,11,15,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,7,12,16,17	6,9,11,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,7,12,14,17,18	6,9,11,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,7,12,14,16	6,9,11	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,7,12,14,17	6,9,11,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,7,12,14,16,18	6,9,11,15,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,7,12,18	6,9,11,13,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,7,12,16,17	6,9,11,13,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,7,12	6,9,11,13,15	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,7,12,16,17,18	6,9,11,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,7,12,14,17	6,9,11,13,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,7,12,14,16,18	6,9,11,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,7,12,14,17,18	6,9,11,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,7,12,14,16	6,9,11,13,15	$2^{-17.5}$

Table 0.1079 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,7,10,18	6,9,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,7,10,16,17	6,9,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,7,10	6,9,15	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,7,10,16,17,18	6,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,7,10,14,17	6,9,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,7,10,14,16,18	6,9,18	2^{-34}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,7,10,14,17,18	6,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,7,10,14,16	6,9,15	2^{-34}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,7,10	6,9,13	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,7,10,16,17,18	6,9,13,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,7,10,18	6,9,13,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,7,10,16,17	6,9,13,15,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,7,10,14,17,18	6,9,13,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,7,10,14,16	6,9,13	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,7,10,14,17	6,9,13,15,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,7,10,14,16,18	6,9,13,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,7,10,12,17	6,9,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,7,10,12,16,18	6,9,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,7,10,12,17,18	6,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,7,10,12,16	6,9,15	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,7,10,12,14,18	6,9,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,7,10,12,14,16,17	6,9,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,7,10,12,14	6,9,15	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,7,10,12,14,16,17,18	6,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,7,10,12,17,18	6,9,13,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,7,10,12,16	6,9,13	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,7,10,12,17	6,9,13,15,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,7,10,12,16,18	6,9,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,7,10,12,14	6,9,13	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,7,10,12,14,16,17,18	6,9,13,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,7,10,12,14,18	6,9,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,7,10,12,14,16,17	6,9,13,15,17	2^{-23}

Table 0.1080 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,7,10	6,9,11	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,7,10,16,17,18	6,9,11,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,7,10,18	6,9,11,15,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,7,10,16,17	6,9,11,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,7,10,14,17,18	6,9,11,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,7,10,14,16	6,9,11	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,7,10,14,17	6,9,11,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,7,10,14,16,18	6,9,11,15,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,7,10,18	6,9,11,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,7,10,16,17	6,9,11,13,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,7,10	6,9,11,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,7,10,16,17,18	6,9,11,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,7,10,14,17	6,9,11,13,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,7,10,14,16,18	6,9,11,13,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,7,10,14,17,18	6,9,11,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,7,10,14,16	6,9,11,13,15	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,7,10,12,17,18	6,9,11,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,7,10,12,16	6,9,11	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,7,10,12,17	6,9,11,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,7,10,12,16,18	6,9,11,15,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,7,10,12,14	6,9,11	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,7,10,12,14,16,17,18	6,9,11,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,7,10,12,14,18	6,9,11,15,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,7,10,12,14,16,17	6,9,11,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,7,10,12,17	6,9,11,13,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,7,10,12,16,18	6,9,11,13,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,7,10,12,17,18	6,9,11,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,7,10,12,16	6,9,11,13,15	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,7,10,12,14,18	6,9,11,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,7,10,12,14,16,17	6,9,11,13,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,7,10,12,14	6,9,11,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,7,10,12,14,16,17,18	6,9,11,13,15,17,18	2^{-23}

Table 0.1081 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,7	6,8	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,7,16,17,18	6,8,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,7,18	6,8,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,7,16,17	6,8,15,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,7,14,17,18	6,8,17,18	2^{-34}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,7,14,16	6,8	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,7,14,17	6,8,15,17	2^{-34}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,7,14,16,18	6,8,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,7,18	6,8,13,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,7,16,17	6,8,13,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,7	6,8,13,15	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,7,16,17,18	6,8,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,7,14,17	6,8,13,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,7,14,16,18	6,8,13,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,7,14,17,18	6,8,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,7,14,16	6,8,13,15	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,7,12,17,18	6,8,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,7,12,16	6,8	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,7,12,17	6,8,15,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,7,12,16,18	6,8,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,7,12,14	6,8	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,7,12,14,16,17,18	6,8,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,7,12,14,18	6,8,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,7,12,14,16,17	6,8,15,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,7,12,17	6,8,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,7,12,16,18	6,8,13,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,7,12,17,18	6,8,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,7,12,16	6,8,13,15	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,7,12,14,18	6,8,13,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,7,12,14,16,17	6,8,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,7,12,14	6,8,13,15	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,7,12,14,16,17,18	6,8,13,15,17,18	$2^{-17.5}$

Table 0.1082 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,7,18	6,8,11,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,7,16,17	6,8,11,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,7	6,8,11,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,7,16,17,18	6,8,11,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,7,14,17	6,8,11,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,7,14,16,18	6,8,11,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,7,14,17,18	6,8,11,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,7,14,16	6,8,11,15	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,7	6,8,11,13	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,7,16,17,18	6,8,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,7,18	6,8,11,13,15,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,7,16,17	6,8,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,7,14,17,18	6,8,11,13,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,7,14,16	6,8,11,13	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,7,14,17	6,8,11,13,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,7,14,16,18	6,8,11,13,15,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,7,12,17	6,8,11,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,7,12,16,18	6,8,11,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,7,12,17,18	6,8,11,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,7,12,16	6,8,11,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,7,12,14,18	6,8,11,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,7,12,14,16,17	6,8,11,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,7,12,14	6,8,11,15	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,7,12,14,16,17,18	6,8,11,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,7,12,17,18	6,8,11,13,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,7,12,16	6,8,11,13	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,7,12,17	6,8,11,13,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,7,12,16,18	6,8,11,13,15,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,7,12,14	6,8,11,13	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,7,12,14,16,17,18	6,8,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,7,12,14,18	6,8,11,13,15,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,7,12,14,16,17	6,8,11,13,15,17	$2^{-17.5}$

Table 0.1083 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,7,10,17,18	6,8,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,7,10,16	6,8	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,7,10,17	6,8,15,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,7,10,16,18	6,8,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,7,10,14	6,8	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,7,10,14,16,17,18	6,8,17,18	2^{-1}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,7,10,14,18	6,8,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,7,10,14,16,17	6,8,15,17	2^{-1}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,7,10,17	6,8,13,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,7,10,16,18	6,8,13,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,7,10,17,18	6,8,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,7,10,16	6,8,13,15	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,7,10,14,18	6,8,13,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,7,10,14,16,17	6,8,13,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,7,10,14	6,8,13,15	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,7,10,14,16,17,18	6,8,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,7,10,12	6,8	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,7,10,12,16,17,18	6,8,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,7,10,12,18	6,8,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,7,10,12,16,17	6,8,15,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,7,10,12,14,17,18	6,8,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,7,10,12,14,16	6,8	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,7,10,12,14,17	6,8,15,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,7,10,12,14,16,18	6,8,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,7,10,12,18	6,8,13,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,7,10,12,16,17	6,8,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,7,10,12	6,8,13,15	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,7,10,12,16,17,18	6,8,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,7,10,12,14,17	6,8,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,7,10,12,14,16,18	6,8,13,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,7,10,12,14,17,18	6,8,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,7,10,12,14,16	6,8,13,15	2^{-12}

Table 0.1084 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,7,10,17	6,8,11,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,7,10,16,18	6,8,11,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,7,10,17,18	6,8,11,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,7,10,16	6,8,11,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,7,10,14,18	6,8,11,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,7,10,14,16,17	6,8,11,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,7,10,14	6,8,11,15	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,7,10,14,16,17,18	6,8,11,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,7,10,17,18	6,8,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,7,10,16	6,8,11,13	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,7,10,17	6,8,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,7,10,16,18	6,8,11,13,15,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,7,10,14	6,8,11,13	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,7,10,14,16,17,18	6,8,11,13,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,7,10,14,18	6,8,11,13,15,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,7,10,14,16,17	6,8,11,13,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,7,10,12,18	6,8,11,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,7,10,12,16,17	6,8,11,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,7,10,12	6,8,11,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,7,10,12,16,17,18	6,8,11,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,7,10,12,14,17	6,8,11,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,7,10,12,14,16,18	6,8,11,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,7,10,12,14,17,18	6,8,11,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,7,10,12,14,16	6,8,11,15	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,7,10,12	6,8,11,13	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,7,10,12,16,17,18	6,8,11,13,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,7,10,12,18	6,8,11,13,15,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,7,10,12,16,17	6,8,11,13,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,7,10,12,14,17,18	6,8,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,7,10,12,14,16	6,8,11,13	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,7,10,12,14,17	6,8,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,7,10,12,14,16,18	6,8,11,13,15,18	2^{-12}

Table 0.1085 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,7,18	6,8,9,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,7,16,17	6,8,9,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,7	6,8,9,15	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,7,16,17,18	6,8,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,7,14,17	6,8,9,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,7,14,16,18	6,8,9,18	2^{-1}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,7,14,17,18	6,8,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,7,14,16	6,8,9,15	2^{-1}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,7	6,8,9,13	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,7,16,17,18	6,8,9,13,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,7,18	6,8,9,13,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,7,16,17	6,8,9,13,15,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,7,14,17,18	6,8,9,13,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,7,14,16	6,8,9,13	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,7,14,17	6,8,9,13,15,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,7,14,16,18	6,8,9,13,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,7,12,17	6,8,9,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,7,12,16,18	6,8,9,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,7,12,17,18	6,8,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,7,12,16	6,8,9,15	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,7,12,14,18	6,8,9,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,7,12,14,16,17	6,8,9,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,7,12,14	6,8,9,15	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,7,12,14,16,17,18	6,8,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,7,12,17,18	6,8,9,13,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,7,12,16	6,8,9,13	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,7,12,17	6,8,9,13,15,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,7,12,16,18	6,8,9,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,7,12,14	6,8,9,13	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,7,12,14,16,17,18	6,8,9,13,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,7,12,14,18	6,8,9,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,7,12,14,16,17	6,8,9,13,15,17	2^{-12}

Table 0.1086 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,7	6,8,9,11	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,7,16,17,18	6,8,9,11,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,7,18	6,8,9,11,15,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,7,16,17	6,8,9,11,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,7,14,17,18	6,8,9,11,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,7,14,16	6,8,9,11	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,7,14,17	6,8,9,11,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,7,14,16,18	6,8,9,11,15,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,7,18	6,8,9,11,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,7,16,17	6,8,9,11,13,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,7	6,8,9,11,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,7,16,17,18	6,8,9,11,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,7,14,17	6,8,9,11,13,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,7,14,16,18	6,8,9,11,13,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,7,14,17,18	6,8,9,11,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,7,14,16	6,8,9,11,13,15	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,7,12,17,18	6,8,9,11,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,7,12,16	6,8,9,11	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,7,12,17	6,8,9,11,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,7,12,16,18	6,8,9,11,15,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,7,12,14	6,8,9,11	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,7,12,14,16,17,18	6,8,9,11,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,7,12,14,18	6,8,9,11,15,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,7,12,14,16,17	6,8,9,11,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,7,12,17	6,8,9,11,13,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,7,12,16,18	6,8,9,11,13,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,7,12,17,18	6,8,9,11,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,7,12,16	6,8,9,11,13,15	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,7,12,14,18	6,8,9,11,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,7,12,14,16,17	6,8,9,11,13,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,7,12,14	6,8,9,11,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,7,12,14,16,17,18	6,8,9,11,13,15,17,18	2^{-12}

Table 0.1087 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,7,10,17	6,8,9,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,7,10,16,18	6,8,9,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,7,10,17,18	6,8,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,7,10,16	6,8,9,15	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,7,10,14,18	6,8,9,18	2^{-34}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,7,10,14,16,17	6,8,9,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,7,10,14	6,8,9,15	2^{-34}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,7,10,14,16,17,18	6,8,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,7,10,17,18	6,8,9,13,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,7,10,16	6,8,9,13	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,7,10,17	6,8,9,13,15,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,7,10,16,18	6,8,9,13,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,7,10,14	6,8,9,13	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,7,10,14,16,17,18	6,8,9,13,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,7,10,14,18	6,8,9,13,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,7,10,14,16,17	6,8,9,13,15,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,7,10,12,18	6,8,9,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,7,10,12,16,17	6,8,9,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,7,10,12	6,8,9,15	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,7,10,12,16,17,18	6,8,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,7,10,12,14,17	6,8,9,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,7,10,12,14,16,18	6,8,9,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,7,10,12,14,17,18	6,8,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,7,10,12,14,16	6,8,9,15	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,7,10,12	6,8,9,13	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,7,10,12,16,17,18	6,8,9,13,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,7,10,12,18	6,8,9,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,7,10,12,16,17	6,8,9,13,15,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,7,10,12,14,17,18	6,8,9,13,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,7,10,12,14,16	6,8,9,13	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,7,10,12,14,17	6,8,9,13,15,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,7,10,12,14,16,18	6,8,9,13,15,18	$2^{-17.5}$

Table 0.1088 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,7,10,17,18	6,8,9,11,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,7,10,16	6,8,9,11	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,7,10,17	6,8,9,11,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,7,10,16,18	6,8,9,11,15,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,7,10,14	6,8,9,11	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,7,10,14,16,17,18	6,8,9,11,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,7,10,14,18	6,8,9,11,15,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,7,10,14,16,17	6,8,9,11,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,7,10,17	6,8,9,11,13,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,7,10,16,18	6,8,9,11,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,7,10,17,18	6,8,9,11,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,7,10,16	6,8,9,11,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,7,10,14,18	6,8,9,11,13,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,7,10,14,16,17	6,8,9,11,13,17	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,7,10,14	6,8,9,11,13,15	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,7,10,14,16,17,18	6,8,9,11,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,7,10,12	6,8,9,11	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,7,10,12,16,17,18	6,8,9,11,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,7,10,12,18	6,8,9,11,15,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,7,10,12,16,17	6,8,9,11,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,7,10,12,14,17,18	6,8,9,11,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,7,10,12,14,16	6,8,9,11	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,7,10,12,14,17	6,8,9,11,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,7,10,12,14,16,18	6,8,9,11,15,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,7,10,12,18	6,8,9,11,13,18	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,7,10,12,16,17	6,8,9,11,13,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,7,10,12	6,8,9,11,13,15	$2^{-28.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,7,10,12,16,17,18	6,8,9,11,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,7,10,12,14,17	6,8,9,11,13,17	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,7,10,12,14,16,18	6,8,9,11,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,7,10,12,14,17,18	6,8,9,11,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,7,10,12,14,16	6,8,9,11,13,15	$2^{-17.5}$

Table 0.1089 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,5	—	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,5,16,17,18	17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,5,18	15,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,5,16,17	15,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,5,14,17,18	17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,5,14,16	—	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,5,14,17	15,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,5,14,16,18	15,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,5,18	13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,5,16,17	13,17	2^{-34}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,5	13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,5,16,17,18	13,15,17,18	2^{-34}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,5,14,17	13,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,5,14,16,18	13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,5,14,17,18	13,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,5,14,16	13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,12,17,18	17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,5,12,16	—	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,12,17	15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,5,12,16,18	15,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,5,12,14	—	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,5,12,14,16,17,18	17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,5,12,14,18	15,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,5,12,14,16,17	15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,12,17	13,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,5,12,16,18	13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,12,17,18	13,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,5,12,16	13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,5,12,14,18	13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,5,12,14,16,17	13,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,5,12,14	13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,5,12,14,16,17,18	13,15,17,18	2^{-23}

Table 0.1090 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,18	11,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,5,16,17	11,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5	11,15	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,16,17,18	11,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,5,14,17	11,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,5,14,16,18	11,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,5,14,17,18	11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,5,14,16	11,15	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,5	11,13	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,5,16,17,18	11,13,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,5,18	11,13,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,5,16,17	11,13,15,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,5,14,17,18	11,13,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,5,14,16	11,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,5,14,17	11,13,15,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,5,14,16,18	11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,5,12,17	11,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,5,12,16,18	11,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,5,12,17,18	11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,5,12,16	11,15	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,5,12,14,18	11,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,5,12,14,16,17	11,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,5,12,14	11,15	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,5,12,14,16,17,18	11,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,5,12,17,18	11,13,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,5,12,16	11,13	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,5,12,17	11,13,15,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,5,12,16,18	11,13,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,5,12,14	11,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,5,12,14,16,17,18	11,13,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,5,12,14,18	11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,5,12,14,16,17	11,13,15,17	2^{-23}

Table 0.1091 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,5,10,17,18	17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,5,10,16	—	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,5,10,17	15,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,5,10,16,18	15,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,5,10,14	—	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,5,10,14,16,17,18	17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,5,10,14,18	15,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,5,10,14,16,17	15,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,5,10,17	13,17	2^{-1}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,5,10,16,18	13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,5,10,17,18	13,15,17,18	2^{-1}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,5,10,16	13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,5,10,14,18	13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,5,10,14,16,17	13,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,5,10,14	13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,5,10,14,16,17,18	13,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,5,10,12	—	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,5,10,12,16,17,18	17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,5,10,12,18	15,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,5,10,12,16,17	15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,5,10,12,14,17,18	17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,5,10,12,14,16	—	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,5,10,12,14,17	15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,5,10,12,14,16,18	15,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,5,10,12,18	13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,5,10,12,16,17	13,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,5,10,12	13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,5,10,12,16,17,18	13,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,5,10,12,14,17	13,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,5,10,12,14,16,18	13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,5,10,12,14,17,18	13,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,5,10,12,14,16	13,15	$2^{-17.5}$

Table 0.1092 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,5,10,17	11,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,5,10,16,18	11,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,5,10,17,18	11,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,5,10,16	11,15	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,5,10,14,18	11,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,5,10,14,16,17	11,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,5,10,14	11,15	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,5,10,14,16,17,18	11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,5,10,17,18	11,13,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,5,10,16	11,13	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,5,10,17	11,13,15,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,5,10,16,18	11,13,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,5,10,14	11,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,5,10,14,16,17,18	11,13,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,5,10,14,18	11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,5,10,14,16,17	11,13,15,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,5,10,12,18	11,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,5,10,12,16,17	11,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,5,10,12	11,15	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,5,10,12,16,17,18	11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,5,10,12,14,17	11,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,5,10,12,14,16,18	11,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,5,10,12,14,17,18	11,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,5,10,12,14,16	11,15	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5,10,12	11,13	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,5,10,12,16,17,18	11,13,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5,10,12,18	11,13,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,5,10,12,16,17	11,13,15,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,5,10,12,14,17,18	11,13,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,5,10,12,14,16	11,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,5,10,12,14,17	11,13,15,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,5,10,12,14,16,18	11,13,15,18	$2^{-17.5}$

Table 0.1093 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,18	9,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,5,16,17	9,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5	9,15	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,5,16,17,18	9,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,14,17	9,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,5,14,16,18	9,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,14,17,18	9,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,5,14,16	9,15	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,5	9,13	2^{-1}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,5,16,17,18	9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,5,18	9,13,15,18	2^{-1}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,5,16,17	9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,14,17,18	9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,5,14,16	9,13	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,14,17	9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,5,14,16,18	9,13,15,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,5,12,17	9,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,5,12,16,18	9,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,5,12,17,18	9,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,5,12,16	9,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,5,12,14,18	9,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,5,12,14,16,17	9,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,5,12,14	9,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,5,12,14,16,17,18	9,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,5,12,17,18	9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,5,12,16	9,13	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,5,12,17	9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,5,12,16,18	9,13,15,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,5,12,14	9,13	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,5,12,14,16,17,18	9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,5,12,14,18	9,13,15,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,5,12,14,16,17	9,13,15,17	$2^{-17.5}$

Table 0.1094 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,5	9,11	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,5,16,17,18	9,11,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,5,18	9,11,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,5,16,17	9,11,15,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,5,14,17,18	9,11,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,5,14,16	9,11	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,5,14,17	9,11,15,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,5,14,16,18	9,11,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,5,18	9,11,13,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,5,16,17	9,11,13,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,5	9,11,13,15	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,5,16,17,18	9,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,5,14,17	9,11,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,5,14,16,18	9,11,13,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,5,14,17,18	9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,5,14,16	9,11,13,15	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,12,17,18	9,11,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,5,12,16	9,11	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,12,17	9,11,15,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,5,12,16,18	9,11,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,5,12,14	9,11	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,5,12,14,16,17,18	9,11,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,5,12,14,18	9,11,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,5,12,14,16,17	9,11,15,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,5,12,17	9,11,13,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,5,12,16,18	9,11,13,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,5,12,17,18	9,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,5,12,16	9,11,13,15	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,5,12,14,18	9,11,13,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,5,12,14,16,17	9,11,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,5,12,14	9,11,13,15	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,5,12,14,16,17,18	9,11,13,15,17,18	$2^{-17.5}$

Table 0.1095 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,5,10,17	9,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,5,10,16,18	9,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,5,10,17,18	9,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,5,10,16	9,15	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,5,10,14,18	9,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,10,14,16,17	9,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,5,10,14	9,15	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,10,14,16,17,18	9,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,5,10,17,18	9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,5,10,16	9,13	2^{-34}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,5,10,17	9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,5,10,16,18	9,13,15,18	2^{-34}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,5,10,14	9,13	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,5,10,14,16,17,18	9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,5,10,14,18	9,13,15,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,5,10,14,16,17	9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,5,10,12,18	9,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,5,10,12,16,17	9,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,5,10,12	9,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,5,10,12,16,17,18	9,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,5,10,12,14,17	9,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,5,10,12,14,16,18	9,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,5,10,12,14,17,18	9,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,5,10,12,14,16	9,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,10,12	9,13	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,5,10,12,16,17,18	9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,10,12,18	9,13,15,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,5,10,12,16,17	9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,5,10,12,14,17,18	9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,5,10,12,14,16	9,13	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,5,10,12,14,17	9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,5,10,12,14,16,18	9,13,15,18	2^{-23}

Table 0.1096 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,5,10,17,18	9,11,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,5,10,16	9,11	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,5,10,17	9,11,15,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,5,10,16,18	9,11,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,5,10,14	9,11	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,5,10,14,16,17,18	9,11,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,5,10,14,18	9,11,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,5,10,14,16,17	9,11,15,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,5,10,17	9,11,13,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,5,10,16,18	9,11,13,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,5,10,17,18	9,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,5,10,16	9,11,13,15	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,5,10,14,18	9,11,13,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,5,10,14,16,17	9,11,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,5,10,14	9,11,13,15	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,5,10,14,16,17,18	9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,5,10,12	9,11	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,5,10,12,16,17,18	9,11,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,5,10,12,18	9,11,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,5,10,12,16,17	9,11,15,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,5,10,12,14,17,18	9,11,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,5,10,12,14,16	9,11	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,5,10,12,14,17	9,11,15,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,5,10,12,14,16,18	9,11,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,5,10,12,18	9,11,13,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,5,10,12,16,17	9,11,13,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,5,10,12	9,11,13,15	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,5,10,12,16,17,18	9,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,5,10,12,14,17	9,11,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,5,10,12,14,16,18	9,11,13,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,10,12,14,17,18	9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,5,10,12,14,16	9,11,13,15	2^{-23}

Table 0.1097 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,5,17,18	8,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,5,16	8	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,5,17	8,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,5,16,18	8,15,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,5,14	8	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,5,14,16,17,18	8,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,5,14,18	8,15,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,5,14,16,17	8,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,5,17	8,13,17	2^{-34}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,16,18	8,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,5,17,18	8,13,15,17,18	2^{-34}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,5,16	8,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,14,18	8,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,5,14,16,17	8,13,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,14	8,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,5,14,16,17,18	8,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,5,12	8	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,5,12,16,17,18	8,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,5,12,18	8,15,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,5,12,16,17	8,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,5,12,14,17,18	8,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,5,12,14,16	8	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,5,12,14,17	8,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,5,12,14,16,18	8,15,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,5,12,18	8,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,12,16,17	8,13,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,5,12	8,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,12,16,17,18	8,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,12,14,17	8,13,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,5,12,14,16,18	8,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,12,14,17,18	8,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,5,12,14,16	8,13,15	$2^{-17.5}$

Table 0.1098 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,5,17	8,11,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,5,16,18	8,11,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,5,17,18	8,11,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,5,16	8,11,15	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,5,14,18	8,11,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,5,14,16,17	8,11,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,5,14	8,11,15	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,5,14,16,17,18	8,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,5,17,18	8,11,13,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,5,16	8,11,13	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,5,17	8,11,13,15,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,5,16,18	8,11,13,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,5,14	8,11,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,5,14,16,17,18	8,11,13,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,5,14,18	8,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,5,14,16,17	8,11,13,15,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,5,12,18	8,11,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,5,12,16,17	8,11,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,5,12	8,11,15	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,5,12,16,17,18	8,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,5,12,14,17	8,11,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,5,12,14,16,18	8,11,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,5,12,14,17,18	8,11,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,5,12,14,16	8,11,15	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,5,12	8,11,13	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,5,12,16,17,18	8,11,13,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,5,12,18	8,11,13,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,5,12,16,17	8,11,13,15,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,5,12,14,17,18	8,11,13,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,5,12,14,16	8,11,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,5,12,14,17	8,11,13,15,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,5,12,14,16,18	8,11,13,15,18	$2^{-17.5}$

Table 0.1099 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,5,10	8	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,10,16,17,18	8,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,5,10,18	8,15,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,10,16,17	8,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,5,10,14,17,18	8,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,10,14,16	8	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,5,10,14,17	8,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,10,14,16,18	8,15,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,5,10,18	8,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,5,10,16,17	8,13,17	2^{-1}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,5,10	8,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,5,10,16,17,18	8,13,15,17,18	2^{-1}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,5,10,14,17	8,13,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,10,14,16,18	8,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,5,10,14,17,18	8,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,10,14,16	8,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,5,10,12,17,18	8,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,5,10,12,16	8	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,5,10,12,17	8,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,5,10,12,16,18	8,15,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,5,10,12,14	8	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,5,10,12,14,16,17,18	8,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,5,10,12,14,18	8,15,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,5,10,12,14,16,17	8,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,5,10,12,17	8,13,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,5,10,12,16,18	8,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,5,10,12,17,18	8,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,5,10,12,16	8,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,5,10,12,14,18	8,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,5,10,12,14,16,17	8,13,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,5,10,12,14	8,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,5,10,12,14,16,17,18	8,13,15,17,18	2^{-12}

Table 0.1100 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,5,10,18	8,11,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,5,10,16,17	8,11,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,5,10	8,11,15	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,5,10,16,17,18	8,11,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,5,10,14,17	8,11,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,5,10,14,16,18	8,11,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,5,10,14,17,18	8,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,5,10,14,16	8,11,15	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,5,10	8,11,13	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,5,10,16,17,18	8,11,13,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,5,10,18	8,11,13,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,5,10,16,17	8,11,13,15,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,5,10,14,17,18	8,11,13,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,5,10,14,16	8,11,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,5,10,14,17	8,11,13,15,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,5,10,14,16,18	8,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,5,10,12,17	8,11,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,10,12,16,18	8,11,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,5,10,12,17,18	8,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,10,12,16	8,11,15	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,5,10,12,14,18	8,11,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,5,10,12,14,16,17	8,11,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,5,10,12,14	8,11,15	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,5,10,12,14,16,17,18	8,11,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,5,10,12,17,18	8,11,13,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,5,10,12,16	8,11,13	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,5,10,12,17	8,11,13,15,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,5,10,12,16,18	8,11,13,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,5,10,12,14	8,11,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,5,10,12,14,16,17,18	8,11,13,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,5,10,12,14,18	8,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,5,10,12,14,16,17	8,11,13,15,17	2^{-12}

Table 0.1101 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,5,17	8,9,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,5,16,18	8,9,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,5,17,18	8,9,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,5,16	8,9,15	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,5,14,18	8,9,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,5,14,16,17	8,9,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,5,14	8,9,15	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,5,14,16,17,18	8,9,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,5,17,18	8,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,5,16	8,9,13	2^{-1}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,5,17	8,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,5,16,18	8,9,13,15,18	2^{-1}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,5,14	8,9,13	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,5,14,16,17,18	8,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,5,14,18	8,9,13,15,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,5,14,16,17	8,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,5,12,18	8,9,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,5,12,16,17	8,9,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,5,12	8,9,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,5,12,16,17,18	8,9,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,5,12,14,17	8,9,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,5,12,14,16,18	8,9,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,5,12,14,17,18	8,9,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,5,12,14,16	8,9,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,5,12	8,9,13	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,5,12,16,17,18	8,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,5,12,18	8,9,13,15,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,5,12,16,17	8,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,5,12,14,17,18	8,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,5,12,14,16	8,9,13	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,5,12,14,17	8,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,5,12,14,16,18	8,9,13,15,18	2^{-12}

Table 0.1102 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,5,17,18	8,9,11,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,5,16	8,9,11	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,5,17	8,9,11,15,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,5,16,18	8,9,11,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,14	8,9,11	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,5,14,16,17,18	8,9,11,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,5,14,18	8,9,11,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,5,14,16,17	8,9,11,15,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,5,17	8,9,11,13,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,5,16,18	8,9,11,13,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,5,17,18	8,9,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,5,16	8,9,11,13,15	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,5,14,18	8,9,11,13,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,5,14,16,17	8,9,11,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,5,14	8,9,11,13,15	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,5,14,16,17,18	8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,5,12	8,9,11	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,5,12,16,17,18	8,9,11,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,5,12,18	8,9,11,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,5,12,16,17	8,9,11,15,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,5,12,14,17,18	8,9,11,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,5,12,14,16	8,9,11	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,5,12,14,17	8,9,11,15,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,5,12,14,16,18	8,9,11,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,5,12,18	8,9,11,13,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5,12,16,17	8,9,11,13,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,5,12	8,9,11,13,15	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5,12,16,17,18	8,9,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,5,12,14,17	8,9,11,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,5,12,14,16,18	8,9,11,13,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,5,12,14,17,18	8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,5,12,14,16	8,9,11,13,15	2^{-12}

Table 0.1103 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,5,10,18	8,9,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,5,10,16,17	8,9,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,5,10	8,9,15	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,5,10,16,17,18	8,9,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,5,10,14,17	8,9,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,5,10,14,16,18	8,9,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,5,10,14,17,18	8,9,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,5,10,14,16	8,9,15	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,5,10	8,9,13	2^{-34}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,5,10,16,17,18	8,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,5,10,18	8,9,13,15,18	2^{-34}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,5,10,16,17	8,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,5,10,14,17,18	8,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,5,10,14,16	8,9,13	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,5,10,14,17	8,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,5,10,14,16,18	8,9,13,15,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,5,10,12,17	8,9,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,10,12,16,18	8,9,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,5,10,12,17,18	8,9,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,10,12,16	8,9,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,5,10,12,14,18	8,9,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,5,10,12,14,16,17	8,9,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,5,10,12,14	8,9,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,5,10,12,14,16,17,18	8,9,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,5,10,12,17,18	8,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,10,12,16	8,9,13	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,5,10,12,17	8,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,10,12,16,18	8,9,13,15,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,5,10,12,14	8,9,13	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,5,10,12,14,16,17,18	8,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,5,10,12,14,18	8,9,13,15,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,5,10,12,14,16,17	8,9,13,15,17	$2^{-17.5}$

Table 0.1104 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,5,10	8,9,11	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,10,16,17,18	8,9,11,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,10,18	8,9,11,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,10,16,17	8,9,11,15,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,5,10,14,17,18	8,9,11,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,5,10,14,16	8,9,11	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,5,10,14,17	8,9,11,15,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,5,10,14,16,18	8,9,11,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,5,10,18	8,9,11,13,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,5,10,16,17	8,9,11,13,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,5,10	8,9,11,13,15	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,5,10,16,17,18	8,9,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,5,10,14,17	8,9,11,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,5,10,14,16,18	8,9,11,13,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,5,10,14,17,18	8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,5,10,14,16	8,9,11,13,15	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,5,10,12,17,18	8,9,11,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,5,10,12,16	8,9,11	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,5,10,12,17	8,9,11,15,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,5,10,12,16,18	8,9,11,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,5,10,12,14	8,9,11	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,5,10,12,14,16,17,18	8,9,11,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,5,10,12,14,18	8,9,11,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,5,10,12,14,16,17	8,9,11,15,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,5,10,12,17	8,9,11,13,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,5,10,12,16,18	8,9,11,13,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,5,10,12,17,18	8,9,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,5,10,12,16	8,9,11,13,15	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,5,10,12,14,18	8,9,11,13,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,5,10,12,14,16,17	8,9,11,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,5,10,12,14	8,9,11,13,15	2^{-23}
$(1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,5,10,12,14,16,17,18	8,9,11,13,15,17,18	$2^{-17.5}$

Table 0.1105 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,5,7,18	18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,5,7,16,17	17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,5,7	15	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,5,7,16,17,18	15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,5,7,14,17	17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,5,7,14,16,18	18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,5,7,14,17,18	15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,5,7,14,16	15	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,5,7	13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,5,7,16,17,18	13,17,18	2^{-34}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,5,7,18	13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,5,7,16,17	13,15,17	2^{-34}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,5,7,14,17,18	13,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,5,7,14,16	13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,5,7,14,17	13,15,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,5,7,14,16,18	13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,5,7,12,17	17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,5,7,12,16,18	18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,5,7,12,17,18	15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,5,7,12,16	15	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,5,7,12,14,18	18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,5,7,12,14,16,17	17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,5,7,12,14	15	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,5,7,12,14,16,17,18	15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,5,7,12,17,18	13,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,5,7,12,16	13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,5,7,12,17	13,15,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,5,7,12,16,18	13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,5,7,12,14	13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,5,7,12,14,16,17,18	13,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,5,7,12,14,18	13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,5,7,12,14,16,17	13,15,17	2^{-23}

Table 0.1106 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,5,7	11	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,5,7,16,17,18	11,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,18	11,15,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,5,7,16,17	11,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,14,17,18	11,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,14,16	11	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,14,17	11,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,14,16,18	11,15,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,5,7,18	11,13,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,5,7,16,17	11,13,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,5,7	11,13,15	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,5,7,16,17,18	11,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,14,17	11,13,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,5,7,14,16,18	11,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,14,17,18	11,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,5,7,14,16	11,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,5,7,12,17,18	11,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,5,7,12,16	11	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,5,7,12,17	11,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,5,7,12,16,18	11,15,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,5,7,12,14	11	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,5,7,12,14,16,17,18	11,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,5,7,12,14,18	11,15,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,5,7,12,14,16,17	11,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,5,7,12,17	11,13,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,5,7,12,16,18	11,13,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,5,7,12,17,18	11,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,5,7,12,16	11,13,15	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,5,7,12,14,18	11,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,5,7,12,14,16,17	11,13,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,5,7,12,14	11,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,5,7,12,14,16,17,18	11,13,15,17,18	2^{-23}

Table 0.1107 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,5,7,10,17	17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,5,7,10,16,18	18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,5,7,10,17,18	15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,5,7,10,16	15	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,5,7,10,14,18	18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,5,7,10,14,16,17	17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,5,7,10,14	15	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,5,7,10,14,16,17,18	15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,5,7,10,17,18	13,17,18	2^{-1}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,5,7,10,16	13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,5,7,10,17	13,15,17	2^{-1}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,5,7,10,16,18	13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,5,7,10,14	13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,5,7,10,14,16,17,18	13,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,5,7,10,14,18	13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,5,7,10,14,16,17	13,15,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,5,7,10,12,18	18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,5,7,10,12,16,17	17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,5,7,10,12	15	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,5,7,10,12,16,17,18	15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,5,7,10,12,14,17	17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,5,7,10,12,14,16,18	18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,5,7,10,12,14,17,18	15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,5,7,10,12,14,16	15	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,5,7,10,12	13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,5,7,10,12,16,17,18	13,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,5,7,10,12,18	13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,5,7,10,12,16,17	13,15,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,5,7,10,12,14,17,18	13,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,5,7,10,12,14,16	13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,5,7,10,12,14,17	13,15,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,5,7,10,12,14,16,18	13,15,18	$2^{-17.5}$

Table 0.1108 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,10,17,18	11,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,5,7,10,16	11	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,10,17	11,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,5,7,10,16,18	11,15,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,5,7,10,14	11	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,7,10,14,16,17,18	11,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,5,7,10,14,18	11,15,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,7,10,14,16,17	11,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,5,7,10,17	11,13,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,5,7,10,16,18	11,13,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,10,17,18	11,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,5,7,10,16	11,13,15	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,5,7,10,14,18	11,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,7,10,14,16,17	11,13,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,5,7,10,14	11,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,7,10,14,16,17,18	11,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,5,7,10,12	11	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,5,7,10,12,16,17,18	11,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,5,7,10,12,18	11,15,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,5,7,10,12,16,17	11,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,5,7,10,12,14,17,18	11,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,10,12,14,16	11	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,5,7,10,12,14,17	11,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,10,12,14,16,18	11,15,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,7,10,12,18	11,13,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,5,7,10,12,16,17	11,13,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,7,10,12	11,13,15	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,5,7,10,12,16,17,18	11,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,5,7,10,12,14,17	11,13,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,5,7,10,12,14,16,18	11,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,5,7,10,12,14,17,18	11,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,7,10,12,14,16	11,13,15	$2^{-17.5}$

Table 0.1109 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,7	9	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,5,7,16,17,18	9,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,7,18	9,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,5,7,16,17	9,15,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,5,7,14,17,18	9,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,5,7,14,16	9	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,5,7,14,17	9,15,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,5,7,14,16,18	9,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,5,7,18	9,13,18	2^{-1}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,5,7,16,17	9,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,5,7	9,13,15	2^{-1}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,5,7,16,17,18	9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,5,7,14,17	9,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,5,7,14,16,18	9,13,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,5,7,14,17,18	9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,5,7,14,16	9,13,15	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,5,7,12,17,18	9,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,5,7,12,16	9	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,5,7,12,17	9,15,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,5,7,12,16,18	9,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,5,7,12,14	9	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,5,7,12,14,16,17,18	9,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,5,7,12,14,18	9,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,5,7,12,14,16,17	9,15,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,5,7,12,17	9,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,5,7,12,16,18	9,13,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,5,7,12,17,18	9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,5,7,12,16	9,13,15	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,5,7,12,14,18	9,13,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,5,7,12,14,16,17	9,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,5,7,12,14	9,13,15	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,5,7,12,14,16,17,18	9,13,15,17,18	$2^{-17.5}$

Table 0.1110 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,5,7,18	9,11,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,5,7,16,17	9,11,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,5,7	9,11,15	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,5,7,16,17,18	9,11,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,5,7,14,17	9,11,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,5,7,14,16,18	9,11,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,5,7,14,17,18	9,11,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,5,7,14,16	9,11,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,5,7	9,11,13	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,5,7,16,17,18	9,11,13,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,5,7,18	9,11,13,15,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,5,7,16,17	9,11,13,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,5,7,14,17,18	9,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,5,7,14,16	9,11,13	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,5,7,14,17	9,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,5,7,14,16,18	9,11,13,15,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,12,17	9,11,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,5,7,12,16,18	9,11,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,12,17,18	9,11,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,5,7,12,16	9,11,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,5,7,12,14,18	9,11,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,5,7,12,14,16,17	9,11,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,5,7,12,14	9,11,15	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,5,7,12,14,16,17,18	9,11,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,7,12,17,18	9,11,13,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,5,7,12,16	9,11,13	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,7,12,17	9,11,13,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,5,7,12,16,18	9,11,13,15,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,5,7,12,14	9,11,13	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,5,7,12,14,16,17,18	9,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,5,7,12,14,18	9,11,13,15,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,5,7,12,14,16,17	9,11,13,15,17	$2^{-17.5}$

Table 0.1111 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,5,7,10,17,18	9,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,5,7,10,16	9	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,5,7,10,17	9,15,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,5,7,10,16,18	9,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,5,7,10,14	9	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,5,7,10,14,16,17,18	9,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,5,7,10,14,18	9,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,5,7,10,14,16,17	9,15,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,10,17	9,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,5,7,10,16,18	9,13,18	2^{-34}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,10,17,18	9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,5,7,10,16	9,13,15	2^{-34}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,5,7,10,14,18	9,13,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,5,7,10,14,16,17	9,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,5,7,10,14	9,13,15	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,5,7,10,14,16,17,18	9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,5,7,10,12	9	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,5,7,10,12,16,17,18	9,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,5,7,10,12,18	9,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,5,7,10,12,16,17	9,15,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,5,7,10,12,14,17,18	9,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,5,7,10,12,14,16	9	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,5,7,10,12,14,17	9,15,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,5,7,10,12,14,16,18	9,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5,7,10,12,18	9,13,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,5,7,10,12,16,17	9,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5,7,10,12	9,13,15	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,5,7,10,12,16,17,18	9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,5,7,10,12,14,17	9,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,5,7,10,12,14,16,18	9,13,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,5,7,10,12,14,17,18	9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,5,7,10,12,14,16	9,13,15	2^{-23}

Table 0.1112 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,5,7,10,17	9,11,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,5,7,10,16,18	9,11,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,5,7,10,17,18	9,11,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,10,16	9,11,15	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,5,7,10,14,18	9,11,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,5,7,10,14,16,17	9,11,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,5,7,10,14	9,11,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,5,7,10,14,16,17,18	9,11,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,5,7,10,17,18	9,11,13,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,5,7,10,16	9,11,13	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,5,7,10,17	9,11,13,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,5,7,10,16,18	9,11,13,15,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,5,7,10,14	9,11,13	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,5,7,10,14,16,17,18	9,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,5,7,10,14,18	9,11,13,15,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,5,7,10,14,16,17	9,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,5,7,10,12,18	9,11,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,5,7,10,12,16,17	9,11,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,7,10,12	9,11,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,5,7,10,12,16,17,18	9,11,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,5,7,10,12,14,17	9,11,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,5,7,10,12,14,16,18	9,11,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,5,7,10,12,14,17,18	9,11,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,5,7,10,12,14,16	9,11,15	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,5,7,10,12	9,11,13	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,5,7,10,12,16,17,18	9,11,13,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,5,7,10,12,18	9,11,13,15,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,5,7,10,12,16,17	9,11,13,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,5,7,10,12,14,17,18	9,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,5,7,10,12,14,16	9,11,13	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,5,7,10,12,14,17	9,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,5,7,10,12,14,16,18	9,11,13,15,18	2^{-23}

Table 0.1113 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,5,7,17	8,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,5,7,16,18	8,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,5,7,17,18	8,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,5,7,16	8,15	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,5,7,14,18	8,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,5,7,14,16,17	8,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,5,7,14	8,15	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,5,7,14,16,17,18	8,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,5,7,17,18	8,13,17,18	2^{-34}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,16	8,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,5,7,17	8,13,15,17	2^{-34}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,16,18	8,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,5,7,14	8,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,5,7,14,16,17,18	8,13,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,5,7,14,18	8,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,5,7,14,16,17	8,13,15,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,5,7,12,18	8,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,5,7,12,16,17	8,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,5,7,12	8,15	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,5,7,12,16,17,18	8,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,5,7,12,14,17	8,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,5,7,12,14,16,18	8,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,5,7,12,14,17,18	8,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,5,7,12,14,16	8,15	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,5,7,12	8,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5,7,12,16,17,18	8,13,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,5,7,12,18	8,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5,7,12,16,17	8,13,15,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,5,7,12,14,17,18	8,13,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,5,7,12,14,16	8,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,5,7,12,14,17	8,13,15,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,5,7,12,14,16,18	8,13,15,18	$2^{-17.5}$

Table 0.1114 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,5,7,17,18	8,11,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,5,7,16	8,11	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,5,7,17	8,11,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,5,7,16,18	8,11,15,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,5,7,14	8,11	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,5,7,14,16,17,18	8,11,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,5,7,14,18	8,11,15,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,5,7,14,16,17	8,11,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,5,7,17	8,11,13,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,5,7,16,18	8,11,13,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,5,7,17,18	8,11,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,5,7,16	8,11,13,15	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,5,7,14,18	8,11,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,5,7,14,16,17	8,11,13,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,5,7,14	8,11,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,5,7,14,16,17,18	8,11,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,5,7,12	8,11	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,5,7,12,16,17,18	8,11,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,5,7,12,18	8,11,15,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,5,7,12,16,17	8,11,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,5,7,12,14,17,18	8,11,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,5,7,12,14,16	8,11	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,5,7,12,14,17	8,11,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,5,7,12,14,16,18	8,11,15,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,5,7,12,18	8,11,13,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,5,7,12,16,17	8,11,13,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,5,7,12	8,11,13,15	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,5,7,12,16,17,18	8,11,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,5,7,12,14,17	8,11,13,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,5,7,12,14,16,18	8,11,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,5,7,12,14,17,18	8,11,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,5,7,12,14,16	8,11,13,15	$2^{-17.5}$

Table 0.1115 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,5,7,10,18	8,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,7,10,16,17	8,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,5,7,10	8,15	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,7,10,16,17,18	8,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,5,7,10,14,17	8,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,5,7,10,14,16,18	8,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,5,7,10,14,17,18	8,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,5,7,10,14,16	8,15	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,5,7,10	8,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,5,7,10,16,17,18	8,13,17,18	2^{-1}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,5,7,10,18	8,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,5,7,10,16,17	8,13,15,17	2^{-1}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,5,7,10,14,17,18	8,13,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,5,7,10,14,16	8,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,5,7,10,14,17	8,13,15,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,5,7,10,14,16,18	8,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,5,7,10,12,17	8,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,5,7,10,12,16,18	8,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,5,7,10,12,17,18	8,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,5,7,10,12,16	8,15	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,5,7,10,12,14,18	8,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,5,7,10,12,14,16,17	8,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,5,7,10,12,14	8,15	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,5,7,10,12,14,16,17,18	8,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,5,7,10,12,17,18	8,13,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,5,7,10,12,16	8,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,5,7,10,12,17	8,13,15,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,5,7,10,12,16,18	8,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,5,7,10,12,14	8,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,5,7,10,12,14,16,17,18	8,13,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,5,7,10,12,14,18	8,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,5,7,10,12,14,16,17	8,13,15,17	2^{-12}

Table 0.1116 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,5,7,10	8,11	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,5,7,10,16,17,18	8,11,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,5,7,10,18	8,11,15,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,5,7,10,16,17	8,11,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,5,7,10,14,17,18	8,11,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,5,7,10,14,16	8,11	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,5,7,10,14,17	8,11,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,5,7,10,14,16,18	8,11,15,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,5,7,10,18	8,11,13,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,5,7,10,16,17	8,11,13,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,5,7,10	8,11,13,15	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,5,7,10,16,17,18	8,11,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,5,7,10,14,17	8,11,13,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,5,7,10,14,16,18	8,11,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,5,7,10,14,17,18	8,11,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,5,7,10,14,16	8,11,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,5,7,10,12,17,18	8,11,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,10,12,16	8,11	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,5,7,10,12,17	8,11,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,10,12,16,18	8,11,15,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,5,7,10,12,14	8,11	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,5,7,10,12,14,16,17,18	8,11,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,5,7,10,12,14,18	8,11,15,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,5,7,10,12,14,16,17	8,11,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,5,7,10,12,17	8,11,13,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,7,10,12,16,18	8,11,13,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,5,7,10,12,17,18	8,11,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,7,10,12,16	8,11,13,15	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,5,7,10,12,14,18	8,11,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,5,7,10,12,14,16,17	8,11,13,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,5,7,10,12,14	8,11,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,5,7,10,12,14,16,17,18	8,11,13,15,17,18	2^{-12}

Table 0.1117 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,5,7,17,18	8,9,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,5,7,16	8,9	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,5,7,17	8,9,15,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,5,7,16,18	8,9,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,5,7,14	8,9	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,5,7,14,16,17,18	8,9,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,5,7,14,18	8,9,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,5,7,14,16,17	8,9,15,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,5,7,17	8,9,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,5,7,16,18	8,9,13,18	2^{-1}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,5,7,17,18	8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,5,7,16	8,9,13,15	2^{-1}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,5,7,14,18	8,9,13,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,5,7,14,16,17	8,9,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,5,7,14	8,9,13,15	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,5,7,14,16,17,18	8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,5,7,12	8,9	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,5,7,12,16,17,18	8,9,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,5,7,12,18	8,9,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,5,7,12,16,17	8,9,15,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,5,7,12,14,17,18	8,9,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,5,7,12,14,16	8,9	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,5,7,12,14,17	8,9,15,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,5,7,12,14,16,18	8,9,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,5,7,12,18	8,9,13,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,12,16,17	8,9,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,5,7,12	8,9,13,15	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,5,7,12,16,17,18	8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,5,7,12,14,17	8,9,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,5,7,12,14,16,18	8,9,13,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,5,7,12,14,17,18	8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,5,7,12,14,16	8,9,13,15	2^{-12}

Table 0.1118 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,5,7,17	8,9,11,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,16,18	8,9,11,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,5,7,17,18	8,9,11,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,16	8,9,11,15	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,7,14,18	8,9,11,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,5,7,14,16,17	8,9,11,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,7,14	8,9,11,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,5,7,14,16,17,18	8,9,11,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,5,7,17,18	8,9,11,13,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,5,7,16	8,9,11,13	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,5,7,17	8,9,11,13,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,5,7,16,18	8,9,11,13,15,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,5,7,14	8,9,11,13	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,5,7,14,16,17,18	8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,5,7,14,18	8,9,11,13,15,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,5,7,14,16,17	8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,5,7,12,18	8,9,11,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,5,7,12,16,17	8,9,11,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,5,7,12	8,9,11,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,5,7,12,16,17,18	8,9,11,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,12,14,17	8,9,11,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,12,14,16,18	8,9,11,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,12,14,17,18	8,9,11,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,12,14,16	8,9,11,15	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,5,7,12	8,9,11,13	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,7,12,16,17,18	8,9,11,13,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,5,7,12,18	8,9,11,13,15,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,7,12,16,17	8,9,11,13,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,5,7,12,14,17,18	8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,5,7,12,14,16	8,9,11,13	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,5,7,12,14,17	8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,5,7,12,14,16,18	8,9,11,13,15,18	2^{-12}

Table 0.1119 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,5,7,10	8,9	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,5,7,10,16,17,18	8,9,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,5,7,10,18	8,9,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,5,7,10,16,17	8,9,15,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,5,7,10,14,17,18	8,9,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,5,7,10,14,16	8,9	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,5,7,10,14,17	8,9,15,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,5,7,10,14,16,18	8,9,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,5,7,10,18	8,9,13,18	2^{-34}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,5,7,10,16,17	8,9,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,5,7,10	8,9,13,15	2^{-34}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,5,7,10,16,17,18	8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,5,7,10,14,17	8,9,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,5,7,10,14,16,18	8,9,13,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,5,7,10,14,17,18	8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,5,7,10,14,16	8,9,13,15	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,5,7,10,12,17,18	8,9,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,5,7,10,12,16	8,9	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,5,7,10,12,17	8,9,15,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,5,7,10,12,16,18	8,9,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,5,7,10,12,14	8,9	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,5,7,10,12,14,16,17,18	8,9,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,5,7,10,12,14,18	8,9,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,5,7,10,12,14,16,17	8,9,15,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,5,7,10,12,17	8,9,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,5,7,10,12,16,18	8,9,13,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,5,7,10,12,17,18	8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,5,7,10,12,16	8,9,13,15	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,5,7,10,12,14,18	8,9,13,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,5,7,10,12,14,16,17	8,9,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,5,7,10,12,14	8,9,13,15	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,5,7,10,12,14,16,17,18	8,9,13,15,17,18	$2^{-17.5}$

Table 0.1120 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,5,7,10,18	8,9,11,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,10,16,17	8,9,11,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,5,7,10	8,9,11,15	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,10,16,17,18	8,9,11,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,10,14,17	8,9,11,17	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,10,14,16,18	8,9,11,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,10,14,17,18	8,9,11,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,10,14,16	8,9,11,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,5,7,10	8,9,11,13	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,5,7,10,16,17,18	8,9,11,13,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,5,7,10,18	8,9,11,13,15,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,5,7,10,16,17	8,9,11,13,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,5,7,10,14,17,18	8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,10,14,16	8,9,11,13	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,5,7,10,14,17	8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,10,14,16,18	8,9,11,13,15,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,5,7,10,12,17	8,9,11,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,5,7,10,12,16,18	8,9,11,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,5,7,10,12,17,18	8,9,11,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,5,7,10,12,16	8,9,11,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,5,7,10,12,14,18	8,9,11,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,5,7,10,12,14,16,17	8,9,11,17	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,5,7,10,12,14	8,9,11,15	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,5,7,10,12,14,16,17,18	8,9,11,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,5,7,10,12,17,18	8,9,11,13,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,5,7,10,12,16	8,9,11,13	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,5,7,10,12,17	8,9,11,13,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,5,7,10,12,16,18	8,9,11,13,15,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,5,7,10,12,14	8,9,11,13	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,5,7,10,12,14,16,17,18	8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,5,7,10,12,14,18	8,9,11,13,15,18	2^{-23}
$(1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,5,7,10,12,14,16,17	8,9,11,13,15,17	$2^{-17.5}$

Table 0.1121 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,5,17,18	6,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,5,16	6	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,5,17	6,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,5,16,18	6,15,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,5,14	6	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,5,14,16,17,18	6,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,5,14,18	6,15,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,5,14,16,17	6,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,5,17	6,13,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,5,16,18	6,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,5,17,18	6,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,5,16	6,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,5,14,18	6,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,5,14,16,17	6,13,17	2^{-34}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,5,14	6,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,5,14,16,17,18	6,13,15,17,18	2^{-34}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,5,12	6	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,5,12,16,17,18	6,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,5,12,18	6,15,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,5,12,16,17	6,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,5,12,14,17,18	6,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,5,12,14,16	6	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,5,12,14,17	6,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,5,12,14,16,18	6,15,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,5,12,18	6,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,5,12,16,17	6,13,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,5,12	6,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,5,12,16,17,18	6,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,5,12,14,17	6,13,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,5,12,14,16,18	6,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,5,12,14,17,18	6,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,5,12,14,16	6,13,15	$2^{-17.5}$

Table 0.1122 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,5,17	6,11,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,5,16,18	6,11,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,5,17,18	6,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,5,16	6,11,15	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,5,14,18	6,11,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,5,14,16,17	6,11,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,5,14	6,11,15	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,5,14,16,17,18	6,11,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,5,17,18	6,11,13,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,5,16	6,11,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,5,17	6,11,13,15,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,5,16,18	6,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5,14	6,11,13	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,5,14,16,17,18	6,11,13,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5,14,18	6,11,13,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,5,14,16,17	6,11,13,15,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,5,12,18	6,11,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,5,12,16,17	6,11,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,5,12	6,11,15	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,12,16,17,18	6,11,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,5,12,14,17	6,11,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,5,12,14,16,18	6,11,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,5,12,14,17,18	6,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,5,12,14,16	6,11,15	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,5,12	6,11,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,5,12,16,17,18	6,11,13,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,5,12,18	6,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,5,12,16,17	6,11,13,15,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,5,12,14,17,18	6,11,13,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,5,12,14,16	6,11,13	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,5,12,14,17	6,11,13,15,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,5,12,14,16,18	6,11,13,15,18	$2^{-28.5}$

Table 0.1123 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,5,10	6	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,5,10,16,17,18	6,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,5,10,18	6,15,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,5,10,16,17	6,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,10,14,17,18	6,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,5,10,14,16	6	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,10,14,17	6,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,5,10,14,16,18	6,15,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,5,10,18	6,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,5,10,16,17	6,13,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,5,10	6,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,5,10,16,17,18	6,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,10,14,17	6,13,17	2^{-1}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,5,10,14,16,18	6,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,10,14,17,18	6,13,15,17,18	2^{-1}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,5,10,14,16	6,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,5,10,12,17,18	6,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,5,10,12,16	6	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,5,10,12,17	6,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,5,10,12,16,18	6,15,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,5,10,12,14	6	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,5,10,12,14,16,17,18	6,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,5,10,12,14,18	6,15,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,5,10,12,14,16,17	6,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,5,10,12,17	6,13,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,5,10,12,16,18	6,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,5,10,12,17,18	6,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,5,10,12,16	6,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,5,10,12,14,18	6,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,5,10,12,14,16,17	6,13,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,5,10,12,14	6,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,5,10,12,14,16,17,18	6,13,15,17,18	2^{-23}

Table 0.1124 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,5,10,18	6,11,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,5,10,16,17	6,11,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,5,10	6,11,15	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,5,10,16,17,18	6,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,5,10,14,17	6,11,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,5,10,14,16,18	6,11,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,5,10,14,17,18	6,11,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,5,10,14,16	6,11,15	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,5,10	6,11,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,5,10,16,17,18	6,11,13,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,5,10,18	6,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,5,10,16,17	6,11,13,15,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,5,10,14,17,18	6,11,13,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,5,10,14,16	6,11,13	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,5,10,14,17	6,11,13,15,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,5,10,14,16,18	6,11,13,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,5,10,12,17	6,11,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,5,10,12,16,18	6,11,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,5,10,12,17,18	6,11,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,5,10,12,16	6,11,15	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,10,12,14,18	6,11,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,5,10,12,14,16,17	6,11,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,10,12,14	6,11,15	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,5,10,12,14,16,17,18	6,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,5,10,12,17,18	6,11,13,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,5,10,12,16	6,11,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,5,10,12,17	6,11,13,15,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,5,10,12,16,18	6,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,5,10,12,14	6,11,13	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,5,10,12,14,16,17,18	6,11,13,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,5,10,12,14,18	6,11,13,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,5,10,12,14,16,17	6,11,13,15,17	2^{-12}

Table 0.1125 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,5,17	6,9,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,5,16,18	6,9,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,5,17,18	6,9,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,5,16	6,9,15	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,5,14,18	6,9,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,5,14,16,17	6,9,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,5,14	6,9,15	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,5,14,16,17,18	6,9,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,5,17,18	6,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,5,16	6,9,13	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,5,17	6,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,5,16,18	6,9,13,15,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,14	6,9,13	2^{-1}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,5,14,16,17,18	6,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,14,18	6,9,13,15,18	2^{-1}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,5,14,16,17	6,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,5,12,18	6,9,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,12,16,17	6,9,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,5,12	6,9,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,12,16,17,18	6,9,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,5,12,14,17	6,9,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,5,12,14,16,18	6,9,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,5,12,14,17,18	6,9,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,5,12,14,16	6,9,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,5,12	6,9,13	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,12,16,17,18	6,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,5,12,18	6,9,13,15,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,12,16,17	6,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,12,14,17,18	6,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,5,12,14,16	6,9,13	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,12,14,17	6,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,5,12,14,16,18	6,9,13,15,18	2^{-23}

Table 0.1126 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,5,17,18	6,9,11,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,5,16	6,9,11	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,5,17	6,9,11,15,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,5,16,18	6,9,11,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,5,14	6,9,11	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,5,14,16,17,18	6,9,11,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,5,14,18	6,9,11,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,5,14,16,17	6,9,11,15,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,5,17	6,9,11,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,5,16,18	6,9,11,13,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,5,17,18	6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,5,16	6,9,11,13,15	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,5,14,18	6,9,11,13,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,5,14,16,17	6,9,11,13,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,5,14	6,9,11,13,15	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,5,14,16,17,18	6,9,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,5,12	6,9,11	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,5,12,16,17,18	6,9,11,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,5,12,18	6,9,11,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,5,12,16,17	6,9,11,15,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,5,12,14,17,18	6,9,11,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,5,12,14,16	6,9,11	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,5,12,14,17	6,9,11,15,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,5,12,14,16,18	6,9,11,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,5,12,18	6,9,11,13,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,5,12,16,17	6,9,11,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,5,12	6,9,11,13,15	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,5,12,16,17,18	6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,5,12,14,17	6,9,11,13,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,5,12,14,16,18	6,9,11,13,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,5,12,14,17,18	6,9,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,5,12,14,16	6,9,11,13,15	2^{-12}

Table 0.1127 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,5,10,18	6,9,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,5,10,16,17	6,9,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,5,10	6,9,15	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,5,10,16,17,18	6,9,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,5,10,14,17	6,9,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,5,10,14,16,18	6,9,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,5,10,14,17,18	6,9,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,5,10,14,16	6,9,15	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,5,10	6,9,13	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,5,10,16,17,18	6,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,5,10,18	6,9,13,15,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,5,10,16,17	6,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,5,10,14,17,18	6,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,5,10,14,16	6,9,13	2^{-34}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,5,10,14,17	6,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,5,10,14,16,18	6,9,13,15,18	2^{-34}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,10,12,17	6,9,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,5,10,12,16,18	6,9,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,10,12,17,18	6,9,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,5,10,12,16	6,9,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,10,12,14,18	6,9,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,5,10,12,14,16,17	6,9,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,10,12,14	6,9,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,5,10,12,14,16,17,18	6,9,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,10,12,17,18	6,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,5,10,12,16	6,9,13	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,10,12,17	6,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,5,10,12,16,18	6,9,13,15,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,5,10,12,14	6,9,13	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,5,10,12,14,16,17,18	6,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,5,10,12,14,18	6,9,13,15,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,5,10,12,14,16,17	6,9,13,15,17	$2^{-17.5}$

Table 0.1128 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,5,10	6,9,11	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,5,10,16,17,18	6,9,11,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,5,10,18	6,9,11,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,5,10,16,17	6,9,11,15,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,5,10,14,17,18	6,9,11,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,5,10,14,16	6,9,11	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,5,10,14,17	6,9,11,15,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,5,10,14,16,18	6,9,11,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,5,10,18	6,9,11,13,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,5,10,16,17	6,9,11,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,5,10	6,9,11,13,15	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,5,10,16,17,18	6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,5,10,14,17	6,9,11,13,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,5,10,14,16,18	6,9,11,13,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,5,10,14,17,18	6,9,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,5,10,14,16	6,9,11,13,15	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,5,10,12,17,18	6,9,11,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,5,10,12,16	6,9,11	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,5,10,12,17	6,9,11,15,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,5,10,12,16,18	6,9,11,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,5,10,12,14	6,9,11	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,5,10,12,14,16,17,18	6,9,11,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,5,10,12,14,18	6,9,11,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,5,10,12,14,16,17	6,9,11,15,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,5,10,12,17	6,9,11,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,5,10,12,16,18	6,9,11,13,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,5,10,12,17,18	6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,5,10,12,16	6,9,11,13,15	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,5,10,12,14,18	6,9,11,13,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,5,10,12,14,16,17	6,9,11,13,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,5,10,12,14	6,9,11,13,15	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,5,10,12,14,16,17,18	6,9,11,13,15,17,18	$2^{-28.5}$

Table 0.1129 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,5	6,8	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,5,16,17,18	6,8,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,5,18	6,8,15,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,5,16,17	6,8,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,5,14,17,18	6,8,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,5,14,16	6,8	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,5,14,17	6,8,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,5,14,16,18	6,8,15,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,5,18	6,8,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,5,16,17	6,8,13,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,5	6,8,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,5,16,17,18	6,8,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,5,14,17	6,8,13,17	2^{-34}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,5,14,16,18	6,8,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,5,14,17,18	6,8,13,15,17,18	2^{-34}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,5,14,16	6,8,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,5,12,17,18	6,8,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,12,16	6,8	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,5,12,17	6,8,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,12,16,18	6,8,15,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,5,12,14	6,8	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,12,14,16,17,18	6,8,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,5,12,14,18	6,8,15,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,12,14,16,17	6,8,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,5,12,17	6,8,13,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,12,16,18	6,8,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,5,12,17,18	6,8,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,12,16	6,8,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,5,12,14,18	6,8,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,5,12,14,16,17	6,8,13,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,5,12,14	6,8,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,5,12,14,16,17,18	6,8,13,15,17,18	2^{-12}

Table 0.1130 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,5,18	6,8,11,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,5,16,17	6,8,11,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,5	6,8,11,15	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,5,16,17,18	6,8,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,5,14,17	6,8,11,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,5,14,16,18	6,8,11,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,5,14,17,18	6,8,11,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,5,14,16	6,8,11,15	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,5	6,8,11,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,5,16,17,18	6,8,11,13,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,5,18	6,8,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,5,16,17	6,8,11,13,15,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,5,14,17,18	6,8,11,13,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,5,14,16	6,8,11,13	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,5,14,17	6,8,11,13,15,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,5,14,16,18	6,8,11,13,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,5,12,17	6,8,11,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,5,12,16,18	6,8,11,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,5,12,17,18	6,8,11,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,5,12,16	6,8,11,15	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,5,12,14,18	6,8,11,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,5,12,14,16,17	6,8,11,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,5,12,14	6,8,11,15	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,5,12,14,16,17,18	6,8,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,5,12,17,18	6,8,11,13,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,5,12,16	6,8,11,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,5,12,17	6,8,11,13,15,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,5,12,16,18	6,8,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,5,12,14	6,8,11,13	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,5,12,14,16,17,18	6,8,11,13,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,5,12,14,18	6,8,11,13,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,5,12,14,16,17	6,8,11,13,15,17	2^{-23}

Table 0.1131 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,5,10,17,18	6,8,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,5,10,16	6,8	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,5,10,17	6,8,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,5,10,16,18	6,8,15,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,5,10,14	6,8	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,5,10,14,16,17,18	6,8,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,5,10,14,18	6,8,15,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,5,10,14,16,17	6,8,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,5,10,17	6,8,13,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,5,10,16,18	6,8,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,5,10,17,18	6,8,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,5,10,16	6,8,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,5,10,14,18	6,8,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,10,14,16,17	6,8,13,17	2^{-1}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,5,10,14	6,8,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,10,14,16,17,18	6,8,13,15,17,18	2^{-1}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,5,10,12	6,8	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,5,10,12,16,17,18	6,8,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,10,12,18	6,8,15,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,5,10,12,16,17	6,8,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,5,10,12,14,17,18	6,8,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,5,10,12,14,16	6,8	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,5,10,12,14,17	6,8,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,5,10,12,14,16,18	6,8,15,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,5,10,12,18	6,8,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,5,10,12,16,17	6,8,13,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,5,10,12	6,8,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,5,10,12,16,17,18	6,8,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,5,10,12,14,17	6,8,13,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,5,10,12,14,16,18	6,8,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,5,10,12,14,17,18	6,8,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,5,10,12,14,16	6,8,13,15	$2^{-17.5}$

Table 0.1132 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,5,10,17	6,8,11,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,5,10,16,18	6,8,11,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,5,10,17,18	6,8,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,5,10,16	6,8,11,15	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,5,10,14,18	6,8,11,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,5,10,14,16,17	6,8,11,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,5,10,14	6,8,11,15	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,5,10,14,16,17,18	6,8,11,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,5,10,17,18	6,8,11,13,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,5,10,16	6,8,11,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,5,10,17	6,8,11,13,15,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,5,10,16,18	6,8,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,5,10,14	6,8,11,13	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,5,10,14,16,17,18	6,8,11,13,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,5,10,14,18	6,8,11,13,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,5,10,14,16,17	6,8,11,13,15,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,5,10,12,18	6,8,11,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,5,10,12,16,17	6,8,11,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,5,10,12	6,8,11,15	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,5,10,12,16,17,18	6,8,11,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,5,10,12,14,17	6,8,11,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,5,10,12,14,16,18	6,8,11,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,5,10,12,14,17,18	6,8,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,5,10,12,14,16	6,8,11,15	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,5,10,12	6,8,11,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,5,10,12,16,17,18	6,8,11,13,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,5,10,12,18	6,8,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,5,10,12,16,17	6,8,11,13,15,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,5,10,12,14,17,18	6,8,11,13,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,5,10,12,14,16	6,8,11,13	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,5,10,12,14,17	6,8,11,13,15,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,5,10,12,14,16,18	6,8,11,13,15,18	$2^{-6.5}$

Table 0.1133 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,5,18	6,8,9,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,5,16,17	6,8,9,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,5	6,8,9,15	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,5,16,17,18	6,8,9,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,5,14,17	6,8,9,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,14,16,18	6,8,9,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,5,14,17,18	6,8,9,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,14,16	6,8,9,15	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,5	6,8,9,13	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,5,16,17,18	6,8,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,5,18	6,8,9,13,15,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,5,16,17	6,8,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,5,14,17,18	6,8,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,14,16	6,8,9,13	2^{-1}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,5,14,17	6,8,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,14,16,18	6,8,9,13,15,18	2^{-1}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,5,12,17	6,8,9,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,5,12,16,18	6,8,9,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,5,12,17,18	6,8,9,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,5,12,16	6,8,9,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,5,12,14,18	6,8,9,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,5,12,14,16,17	6,8,9,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,5,12,14	6,8,9,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,5,12,14,16,17,18	6,8,9,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,5,12,17,18	6,8,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,5,12,16	6,8,9,13	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,5,12,17	6,8,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,5,12,16,18	6,8,9,13,15,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,5,12,14	6,8,9,13	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,5,12,14,16,17,18	6,8,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,5,12,14,18	6,8,9,13,15,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,5,12,14,16,17	6,8,9,13,15,17	$2^{-17.5}$

Table 0.1134 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,5	6,8,9,11	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,5,16,17,18	6,8,9,11,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,5,18	6,8,9,11,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,5,16,17	6,8,9,11,15,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,5,14,17,18	6,8,9,11,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,5,14,16	6,8,9,11	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,5,14,17	6,8,9,11,15,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,5,14,16,18	6,8,9,11,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,5,18	6,8,9,11,13,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,5,16,17	6,8,9,11,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,5	6,8,9,11,13,15	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,5,16,17,18	6,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,5,14,17	6,8,9,11,13,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,5,14,16,18	6,8,9,11,13,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,5,14,17,18	6,8,9,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,5,14,16	6,8,9,11,13,15	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,5,12,17,18	6,8,9,11,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,5,12,16	6,8,9,11	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,5,12,17	6,8,9,11,15,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,5,12,16,18	6,8,9,11,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,5,12,14	6,8,9,11	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,12,14,16,17,18	6,8,9,11,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,5,12,14,18	6,8,9,11,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,5,12,14,16,17	6,8,9,11,15,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,5,12,17	6,8,9,11,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,5,12,16,18	6,8,9,11,13,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,5,12,17,18	6,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,5,12,16	6,8,9,11,13,15	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,5,12,14,18	6,8,9,11,13,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,5,12,14,16,17	6,8,9,11,13,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,5,12,14	6,8,9,11,13,15	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,5,12,14,16,17,18	6,8,9,11,13,15,17,18	$2^{-6.5}$

Table 0.1135 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,5,10,17	6,8,9,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,5,10,16,18	6,8,9,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,5,10,17,18	6,8,9,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,5,10,16	6,8,9,15	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,5,10,14,18	6,8,9,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,5,10,14,16,17	6,8,9,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,5,10,14	6,8,9,15	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,5,10,14,16,17,18	6,8,9,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,5,10,17,18	6,8,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,5,10,16	6,8,9,13	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,5,10,17	6,8,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,5,10,16,18	6,8,9,13,15,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,5,10,14	6,8,9,13	2^{-34}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,5,10,14,16,17,18	6,8,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,5,10,14,18	6,8,9,13,15,18	2^{-34}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,5,10,14,16,17	6,8,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,5,10,12,18	6,8,9,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,5,10,12,16,17	6,8,9,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,5,10,12	6,8,9,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,5,10,12,16,17,18	6,8,9,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,5,10,12,14,17	6,8,9,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,5,10,12,14,16,18	6,8,9,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,5,10,12,14,17,18	6,8,9,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,5,10,12,14,16	6,8,9,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,5,10,12	6,8,9,13	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,5,10,12,16,17,18	6,8,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,5,10,12,18	6,8,9,13,15,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,5,10,12,16,17	6,8,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,5,10,12,14,17,18	6,8,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,5,10,12,14,16	6,8,9,13	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,5,10,12,14,17	6,8,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,5,10,12,14,16,18	6,8,9,13,15,18	2^{-12}

Table 0.1136 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,5,10,17,18	6,8,9,11,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,5,10,16	6,8,9,11	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,5,10,17	6,8,9,11,15,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,5,10,16,18	6,8,9,11,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,5,10,14	6,8,9,11	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,5,10,14,16,17,18	6,8,9,11,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,5,10,14,18	6,8,9,11,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,5,10,14,16,17	6,8,9,11,15,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,5,10,17	6,8,9,11,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,5,10,16,18	6,8,9,11,13,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,5,10,17,18	6,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,5,10,16	6,8,9,11,13,15	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,5,10,14,18	6,8,9,11,13,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5,10,14,16,17	6,8,9,11,13,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,5,10,14	6,8,9,11,13,15	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5,10,14,16,17,18	6,8,9,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,10,12	6,8,9,11	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,5,10,12,16,17,18	6,8,9,11,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,10,12,18	6,8,9,11,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,5,10,12,16,17	6,8,9,11,15,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,5,10,12,14,17,18	6,8,9,11,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,5,10,12,14,16	6,8,9,11	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,5,10,12,14,17	6,8,9,11,15,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,5,10,12,14,16,18	6,8,9,11,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,5,10,12,18	6,8,9,11,13,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,5,10,12,16,17	6,8,9,11,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,5,10,12	6,8,9,11,13,15	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,5,10,12,16,17,18	6,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,5,10,12,14,17	6,8,9,11,13,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,5,10,12,14,16,18	6,8,9,11,13,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,5,10,12,14,17,18	6,8,9,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,5,10,12,14,16	6,8,9,11,13,15	2^{-23}

Table 0.1137 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,5,7,17	6,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,5,7,16,18	6,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,5,7,17,18	6,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,5,7,16	6,15	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,5,7,14,18	6,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,5,7,14,16,17	6,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,5,7,14	6,15	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,5,7,14,16,17,18	6,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,5,7,17,18	6,13,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,5,7,16	6,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,5,7,17	6,13,15,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,5,7,16,18	6,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,5,7,14	6,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,5,7,14,16,17,18	6,13,17,18	2^{-34}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,5,7,14,18	6,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,5,7,14,16,17	6,13,15,17	2^{-34}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,5,7,12,18	6,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,5,7,12,16,17	6,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,5,7,12	6,15	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,5,7,12,16,17,18	6,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,5,7,12,14,17	6,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,5,7,12,14,16,18	6,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,5,7,12,14,17,18	6,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,5,7,12,14,16	6,15	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,5,7,12	6,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,5,7,12,16,17,18	6,13,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,5,7,12,18	6,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,5,7,12,16,17	6,13,15,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,5,7,12,14,17,18	6,13,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,5,7,12,14,16	6,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,5,7,12,14,17	6,13,15,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,5,7,12,14,16,18	6,13,15,18	$2^{-17.5}$

Table 0.1138 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,17,18	6,11,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,16	6,11	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,17	6,11,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,16,18	6,11,15,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,5,7,14	6,11	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,5,7,14,16,17,18	6,11,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,5,7,14,18	6,11,15,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,5,7,14,16,17	6,11,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,5,7,17	6,11,13,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,5,7,16,18	6,11,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,5,7,17,18	6,11,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,5,7,16	6,11,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,7,14,18	6,11,13,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,5,7,14,16,17	6,11,13,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,7,14	6,11,13,15	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,5,7,14,16,17,18	6,11,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,5,7,12	6,11	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,7,12,16,17,18	6,11,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,5,7,12,18	6,11,15,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,7,12,16,17	6,11,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,12,14,17,18	6,11,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,5,7,12,14,16	6,11	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,12,14,17	6,11,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,5,7,12,14,16,18	6,11,15,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,5,7,12,18	6,11,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,5,7,12,16,17	6,11,13,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,5,7,12	6,11,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,5,7,12,16,17,18	6,11,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,5,7,12,14,17	6,11,13,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,5,7,12,14,16,18	6,11,13,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,5,7,12,14,17,18	6,11,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,5,7,12,14,16	6,11,13,15	$2^{-28.5}$

Table 0.1139 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,5,7,10,18	6,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,5,7,10,16,17	6,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,5,7,10	6,15	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,5,7,10,16,17,18	6,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,5,7,10,14,17	6,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,5,7,10,14,16,18	6,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,5,7,10,14,17,18	6,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,5,7,10,14,16	6,15	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,5,7,10	6,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,5,7,10,16,17,18	6,13,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,5,7,10,18	6,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,5,7,10,16,17	6,13,15,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,5,7,10,14,17,18	6,13,17,18	2^{-1}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,5,7,10,14,16	6,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,5,7,10,14,17	6,13,15,17	2^{-1}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,5,7,10,14,16,18	6,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,5,7,10,12,17	6,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,5,7,10,12,16,18	6,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,5,7,10,12,17,18	6,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,5,7,10,12,16	6,15	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,5,7,10,12,14,18	6,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,5,7,10,12,14,16,17	6,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,5,7,10,12,14	6,15	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,5,7,10,12,14,16,17,18	6,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,5,7,10,12,17,18	6,13,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,5,7,10,12,16	6,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,5,7,10,12,17	6,13,15,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,5,7,10,12,16,18	6,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,5,7,10,12,14	6,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,5,7,10,12,14,16,17,18	6,13,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,5,7,10,12,14,18	6,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,5,7,10,12,14,16,17	6,13,15,17	2^{-23}

Table 0.1140 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,5,7,10	6,11	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,5,7,10,16,17,18	6,11,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,5,7,10,18	6,11,15,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,5,7,10,16,17	6,11,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,5,7,10,14,17,18	6,11,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,5,7,10,14,16	6,11	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,5,7,10,14,17	6,11,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,5,7,10,14,16,18	6,11,15,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,5,7,10,18	6,11,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,5,7,10,16,17	6,11,13,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,5,7,10	6,11,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,5,7,10,16,17,18	6,11,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,5,7,10,14,17	6,11,13,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,5,7,10,14,16,18	6,11,13,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,5,7,10,14,17,18	6,11,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,5,7,10,14,16	6,11,13,15	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,10,12,17,18	6,11,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,10,12,16	6,11	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,10,12,17	6,11,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,10,12,16,18	6,11,15,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,10,12,14	6,11	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,5,7,10,12,14,16,17,18	6,11,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,10,12,14,18	6,11,15,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,5,7,10,12,14,16,17	6,11,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,5,7,10,12,17	6,11,13,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,5,7,10,12,16,18	6,11,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,10,12,17,18	6,11,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,5,7,10,12,16	6,11,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,5,7,10,12,14,18	6,11,13,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,5,7,10,12,14,16,17	6,11,13,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,5,7,10,12,14	6,11,13,15	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,5,7,10,12,14,16,17,18	6,11,13,15,17,18	2^{-12}

Table 0.1141 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,5,7,17,18	6,9,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,5,7,16	6,9	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,5,7,17	6,9,15,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,5,7,16,18	6,9,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,5,7,14	6,9	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,5,7,14,16,17,18	6,9,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,5,7,14,18	6,9,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,5,7,14,16,17	6,9,15,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,5,7,17	6,9,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,5,7,16,18	6,9,13,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,5,7,17,18	6,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,5,7,16	6,9,13,15	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5,7,14,18	6,9,13,18	2^{-1}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,5,7,14,16,17	6,9,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5,7,14	6,9,13,15	2^{-1}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,5,7,14,16,17,18	6,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,5,7,12	6,9	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,5,7,12,16,17,18	6,9,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,5,7,12,18	6,9,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,5,7,12,16,17	6,9,15,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,5,7,12,14,17,18	6,9,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,5,7,12,14,16	6,9	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,5,7,12,14,17	6,9,15,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,5,7,12,14,16,18	6,9,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,5,7,12,18	6,9,13,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,5,7,12,16,17	6,9,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,5,7,12	6,9,13,15	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,5,7,12,16,17,18	6,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,12,14,17	6,9,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,5,7,12,14,16,18	6,9,13,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,12,14,17,18	6,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,5,7,12,14,16	6,9,13,15	2^{-23}

Table 0.1142 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,5,7,17	6,9,11,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,5,7,16,18	6,9,11,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,5,7,17,18	6,9,11,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,5,7,16	6,9,11,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,5,7,14,18	6,9,11,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,5,7,14,16,17	6,9,11,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,5,7,14	6,9,11,15	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,5,7,14,16,17,18	6,9,11,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,5,7,17,18	6,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,5,7,16	6,9,11,13	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,5,7,17	6,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,5,7,16,18	6,9,11,13,15,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,5,7,14	6,9,11,13	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,5,7,14,16,17,18	6,9,11,13,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,5,7,14,18	6,9,11,13,15,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,5,7,14,16,17	6,9,11,13,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,5,7,12,18	6,9,11,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,5,7,12,16,17	6,9,11,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,5,7,12	6,9,11,15	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,5,7,12,16,17,18	6,9,11,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,5,7,12,14,17	6,9,11,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,5,7,12,14,16,18	6,9,11,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,5,7,12,14,17,18	6,9,11,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,5,7,12,14,16	6,9,11,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,5,7,12	6,9,11,13	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,5,7,12,16,17,18	6,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,5,7,12,18	6,9,11,13,15,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,5,7,12,16,17	6,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,5,7,12,14,17,18	6,9,11,13,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,5,7,12,14,16	6,9,11,13	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,5,7,12,14,17	6,9,11,13,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,5,7,12,14,16,18	6,9,11,13,15,18	2^{-12}

Table 0.1143 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,5,7,10	6,9	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,5,7,10,16,17,18	6,9,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,5,7,10,18	6,9,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,5,7,10,16,17	6,9,15,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,5,7,10,14,17,18	6,9,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,5,7,10,14,16	6,9	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,5,7,10,14,17	6,9,15,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,5,7,10,14,16,18	6,9,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,5,7,10,18	6,9,13,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,5,7,10,16,17	6,9,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,5,7,10	6,9,13,15	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,5,7,10,16,17,18	6,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,5,7,10,14,17	6,9,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,5,7,10,14,16,18	6,9,13,18	2^{-34}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,5,7,10,14,17,18	6,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,5,7,10,14,16	6,9,13,15	2^{-34}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,5,7,10,12,17,18	6,9,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,5,7,10,12,16	6,9	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,5,7,10,12,17	6,9,15,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,5,7,10,12,16,18	6,9,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,5,7,10,12,14	6,9	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,5,7,10,12,14,16,17,18	6,9,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,7,10,12,14,18	6,9,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,5,7,10,12,14,16,17	6,9,15,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,5,7,10,12,17	6,9,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,5,7,10,12,16,18	6,9,13,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,5,7,10,12,17,18	6,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,5,7,10,12,16	6,9,13,15	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,5,7,10,12,14,18	6,9,13,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,5,7,10,12,14,16,17	6,9,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,5,7,10,12,14	6,9,13,15	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,5,7,10,12,14,16,17,18	6,9,13,15,17,18	$2^{-17.5}$

Table 0.1144 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,5,7,10,18	6,9,11,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,5,7,10,16,17	6,9,11,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,5,7,10	6,9,11,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,5,7,10,16,17,18	6,9,11,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,10,14,17	6,9,11,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,5,7,10,14,16,18	6,9,11,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,10,14,17,18	6,9,11,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,5,7,10,14,16	6,9,11,15	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,5,7,10	6,9,11,13	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,5,7,10,16,17,18	6,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,5,7,10,18	6,9,11,13,15,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,5,7,10,16,17	6,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,7,10,14,17,18	6,9,11,13,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,5,7,10,14,16	6,9,11,13	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,7,10,14,17	6,9,11,13,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,5,7,10,14,16,18	6,9,11,13,15,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,5,7,10,12,17	6,9,11,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,5,7,10,12,16,18	6,9,11,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,5,7,10,12,17,18	6,9,11,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,5,7,10,12,16	6,9,11,15	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,5,7,10,12,14,18	6,9,11,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,5,7,10,12,14,16,17	6,9,11,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,5,7,10,12,14	6,9,11,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,5,7,10,12,14,16,17,18	6,9,11,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,5,7,10,12,17,18	6,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,5,7,10,12,16	6,9,11,13	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,7,10,12,17	6,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,5,7,10,12,16,18	6,9,11,13,15,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,5,7,10,12,14	6,9,11,13	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,5,7,10,12,14,16,17,18	6,9,11,13,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,5,7,10,12,14,18	6,9,11,13,15,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,5,7,10,12,14,16,17	6,9,11,13,15,17	$2^{-28.5}$

Table 0.1145 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,5,7,18	6,8,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,5,7,16,17	6,8,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,5,7	6,8,15	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,5,7,16,17,18	6,8,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,5,7,14,17	6,8,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,5,7,14,16,18	6,8,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,5,7,14,17,18	6,8,15,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,5,7,14,16	6,8,15	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,5,7	6,8,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,5,7,16,17,18	6,8,13,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,5,7,18	6,8,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,5,7,16,17	6,8,13,15,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,5,7,14,17,18	6,8,13,17,18	2^{-34}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,5,7,14,16	6,8,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,5,7,14,17	6,8,13,15,17	2^{-34}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,5,7,14,16,18	6,8,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,5,7,12,17	6,8,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,5,7,12,16,18	6,8,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,5,7,12,17,18	6,8,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,5,7,12,16	6,8,15	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,5,7,12,14,18	6,8,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,7,12,14,16,17	6,8,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,5,7,12,14	6,8,15	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,7,12,14,16,17,18	6,8,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,5,7,12,17,18	6,8,13,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,5,7,12,16	6,8,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,5,7,12,17	6,8,13,15,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,5,7,12,16,18	6,8,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,5,7,12,14	6,8,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,5,7,12,14,16,17,18	6,8,13,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,5,7,12,14,18	6,8,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,5,7,12,14,16,17	6,8,13,15,17	2^{-12}

Table 0.1146 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,5,7	6,8,11	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,5,7,16,17,18	6,8,11,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,5,7,18	6,8,11,15,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,5,7,16,17	6,8,11,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,5,7,14,17,18	6,8,11,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,14,16	6,8,11	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,5,7,14,17	6,8,11,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,14,16,18	6,8,11,15,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,5,7,18	6,8,11,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,5,7,16,17	6,8,11,13,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,5,7	6,8,11,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,5,7,16,17,18	6,8,11,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,5,7,14,17	6,8,11,13,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,7,14,16,18	6,8,11,13,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,5,7,14,17,18	6,8,11,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,7,14,16	6,8,11,13,15	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,5,7,12,17,18	6,8,11,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,5,7,12,16	6,8,11	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,5,7,12,17	6,8,11,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,5,7,12,16,18	6,8,11,15,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,5,7,12,14	6,8,11	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,5,7,12,14,16,17,18	6,8,11,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,5,7,12,14,18	6,8,11,15,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,5,7,12,14,16,17	6,8,11,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,5,7,12,17	6,8,11,13,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,5,7,12,16,18	6,8,11,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,5,7,12,17,18	6,8,11,13,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,5,7,12,16	6,8,11,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,5,7,12,14,18	6,8,11,13,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,5,7,12,14,16,17	6,8,11,13,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,5,7,12,14	6,8,11,13,15	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,5,7,12,14,16,17,18	6,8,11,13,15,17,18	2^{-23}

Table 0.1147 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,5,7,10,17	6,8,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,5,7,10,16,18	6,8,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,5,7,10,17,18	6,8,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,5,7,10,16	6,8,15	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,5,7,10,14,18	6,8,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,5,7,10,14,16,17	6,8,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,5,7,10,14	6,8,15	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,5,7,10,14,16,17,18	6,8,15,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,5,7,10,17,18	6,8,13,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,5,7,10,16	6,8,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,5,7,10,17	6,8,13,15,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,5,7,10,16,18	6,8,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,5,7,10,14	6,8,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5,7,10,14,16,17,18	6,8,13,17,18	2^{-1}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,5,7,10,14,18	6,8,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5,7,10,14,16,17	6,8,13,15,17	2^{-1}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,7,10,12,18	6,8,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,5,7,10,12,16,17	6,8,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,5,7,10,12	6,8,15	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,5,7,10,12,16,17,18	6,8,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,5,7,10,12,14,17	6,8,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,5,7,10,12,14,16,18	6,8,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,5,7,10,12,14,17,18	6,8,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,5,7,10,12,14,16	6,8,15	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,5,7,10,12	6,8,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,5,7,10,12,16,17,18	6,8,13,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,5,7,10,12,18	6,8,13,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,5,7,10,12,16,17	6,8,13,15,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,5,7,10,12,14,17,18	6,8,13,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,10,12,14,16	6,8,13	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,5,7,10,12,14,17	6,8,13,15,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,10,12,14,16,18	6,8,13,15,18	$2^{-17.5}$

Table 0.1148 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,5,7,10,17,18	6,8,11,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,5,7,10,16	6,8,11	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,5,7,10,17	6,8,11,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,5,7,10,16,18	6,8,11,15,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,5,7,10,14	6,8,11	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,5,7,10,14,16,17,18	6,8,11,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,5,7,10,14,18	6,8,11,15,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,5,7,10,14,16,17	6,8,11,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,5,7,10,17	6,8,11,13,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,5,7,10,16,18	6,8,11,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,5,7,10,17,18	6,8,11,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,5,7,10,16	6,8,11,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,5,7,10,14,18	6,8,11,13,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,5,7,10,14,16,17	6,8,11,13,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,5,7,10,14	6,8,11,13,15	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,5,7,10,14,16,17,18	6,8,11,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,5,7,10,12	6,8,11	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,5,7,10,12,16,17,18	6,8,11,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,5,7,10,12,18	6,8,11,15,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,5,7,10,12,16,17	6,8,11,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,5,7,10,12,14,17,18	6,8,11,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,5,7,10,12,14,16	6,8,11	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,5,7,10,12,14,17	6,8,11,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,5,7,10,12,14,16,18	6,8,11,15,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,5,7,10,12,18	6,8,11,13,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,5,7,10,12,16,17	6,8,11,13,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,5,7,10,12	6,8,11,13,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,5,7,10,12,16,17,18	6,8,11,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,5,7,10,12,14,17	6,8,11,13,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,5,7,10,12,14,16,18	6,8,11,13,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,5,7,10,12,14,17,18	6,8,11,13,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,5,7,10,12,14,16	6,8,11,13,15	$2^{-6.5}$

Table 0.1149 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,5,7	6,8,9	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,5,7,16,17,18	6,8,9,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,5,7,18	6,8,9,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,5,7,16,17	6,8,9,15,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,5,7,14,17,18	6,8,9,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,5,7,14,16	6,8,9	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,5,7,14,17	6,8,9,15,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,5,7,14,16,18	6,8,9,15,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,5,7,18	6,8,9,13,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,5,7,16,17	6,8,9,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,5,7	6,8,9,13,15	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,5,7,16,17,18	6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,5,7,14,17	6,8,9,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,5,7,14,16,18	6,8,9,13,18	2^{-1}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,5,7,14,17,18	6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,5,7,14,16	6,8,9,13,15	2^{-1}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,5,7,12,17,18	6,8,9,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,5,7,12,16	6,8,9	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,5,7,12,17	6,8,9,15,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,5,7,12,16,18	6,8,9,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,5,7,12,14	6,8,9	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,5,7,12,14,16,17,18	6,8,9,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,5,7,12,14,18	6,8,9,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,5,7,12,14,16,17	6,8,9,15,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,5,7,12,17	6,8,9,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,5,7,12,16,18	6,8,9,13,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,5,7,12,17,18	6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,5,7,12,16	6,8,9,13,15	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,5,7,12,14,18	6,8,9,13,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,5,7,12,14,16,17	6,8,9,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,5,7,12,14	6,8,9,13,15	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,5,7,12,14,16,17,18	6,8,9,13,15,17,18	$2^{-17.5}$

Table 0.1150 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,5,7,18	6,8,9,11,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,5,7,16,17	6,8,9,11,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,5,7	6,8,9,11,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,5,7,16,17,18	6,8,9,11,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,5,7,14,17	6,8,9,11,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,5,7,14,16,18	6,8,9,11,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,5,7,14,17,18	6,8,9,11,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,5,7,14,16	6,8,9,11,15	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,5,7	6,8,9,11,13	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,5,7,16,17,18	6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,5,7,18	6,8,9,11,13,15,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,5,7,16,17	6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,5,7,14,17,18	6,8,9,11,13,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,5,7,14,16	6,8,9,11,13	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,5,7,14,17	6,8,9,11,13,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,5,7,14,16,18	6,8,9,11,13,15,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,12,17	6,8,9,11,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,12,16,18	6,8,9,11,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,12,17,18	6,8,9,11,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,12,16	6,8,9,11,15	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,5,7,12,14,18	6,8,9,11,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,12,14,16,17	6,8,9,11,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,5,7,12,14	6,8,9,11,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,12,14,16,17,18	6,8,9,11,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,5,7,12,17,18	6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,12,16	6,8,9,11,13	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,5,7,12,17	6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,12,16,18	6,8,9,11,13,15,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,5,7,12,14	6,8,9,11,13	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,5,7,12,14,16,17,18	6,8,9,11,13,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,5,7,12,14,18	6,8,9,11,13,15,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,5,7,12,14,16,17	6,8,9,11,13,15,17	$2^{-6.5}$

Table 0.1151 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,5,7,10,17,18	6,8,9,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,5,7,10,16	6,8,9	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,5,7,10,17	6,8,9,15,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,5,7,10,16,18	6,8,9,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,5,7,10,14	6,8,9	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,5,7,10,14,16,17,18	6,8,9,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,5,7,10,14,18	6,8,9,15,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,5,7,10,14,16,17	6,8,9,15,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,5,7,10,17	6,8,9,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,5,7,10,16,18	6,8,9,13,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,5,7,10,17,18	6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,5,7,10,16	6,8,9,13,15	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,5,7,10,14,18	6,8,9,13,18	2^{-34}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,5,7,10,14,16,17	6,8,9,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,5,7,10,14	6,8,9,13,15	2^{-34}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,5,7,10,14,16,17,18	6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,5,7,10,12	6,8,9	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,5,7,10,12,16,17,18	6,8,9,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,5,7,10,12,18	6,8,9,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,5,7,10,12,16,17	6,8,9,15,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,5,7,10,12,14,17,18	6,8,9,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,5,7,10,12,14,16	6,8,9	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,5,7,10,12,14,17	6,8,9,15,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,5,7,10,12,14,16,18	6,8,9,15,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,5,7,10,12,18	6,8,9,13,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,5,7,10,12,16,17	6,8,9,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,5,7,10,12	6,8,9,13,15	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,5,7,10,12,16,17,18	6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,5,7,10,12,14,17	6,8,9,13,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,5,7,10,12,14,16,18	6,8,9,13,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,5,7,10,12,14,17,18	6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,5,7,10,12,14,16	6,8,9,13,15	2^{-12}

Table 0.1152 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,10,17	6,8,9,11,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,10,16,18	6,8,9,11,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,10,17,18	6,8,9,11,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,10,16	6,8,9,11,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,5,7,10,14,18	6,8,9,11,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,5,7,10,14,16,17	6,8,9,11,17	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,5,7,10,14	6,8,9,11,15	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,5,7,10,14,16,17,18	6,8,9,11,15,17,18	2^{-12}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,5,7,10,17,18	6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,5,7,10,16	6,8,9,11,13	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,5,7,10,17	6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,5,7,10,16,18	6,8,9,11,13,15,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,5,7,10,14	6,8,9,11,13	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,7,10,14,16,17,18	6,8,9,11,13,17,18	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,5,7,10,14,18	6,8,9,11,13,15,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,7,10,14,16,17	6,8,9,11,13,15,17	$2^{-6.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,7,10,12,18	6,8,9,11,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,5,7,10,12,16,17	6,8,9,11,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,7,10,12	6,8,9,11,15	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,5,7,10,12,16,17,18	6,8,9,11,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,5,7,10,12,14,17	6,8,9,11,17	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,10,12,14,16,18	6,8,9,11,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,5,7,10,12,14,17,18	6,8,9,11,15,17,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,10,12,14,16	6,8,9,11,15	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,5,7,10,12	6,8,9,11,13	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,5,7,10,12,16,17,18	6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,5,7,10,12,18	6,8,9,11,13,15,18	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,5,7,10,12,16,17	6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,5,7,10,12,14,17,18	6,8,9,11,13,17,18	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,10,12,14,16	6,8,9,11,13	2^{-23}
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,5,7,10,12,14,17	6,8,9,11,13,15,17	$2^{-28.5}$
$(1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,5,7,10,12,14,16,18	6,8,9,11,13,15,18	2^{-23}

Table 0.1153 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,17	4,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,16,18	4,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,17,18	4,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,16	4,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,14,18	4,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,14,16,17	4,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,14	4,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,14,16,17,18	4,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,17,18	4,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,16	4,13	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,17	4,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,16,18	4,13,15,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,14	4,13	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,14,16,17,18	4,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,14,18	4,13,15,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,14,16,17	4,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,12,18	4,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,12,16,17	4,17	2^{-34}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,12	4,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,12,16,17,18	4,15,17,18	2^{-34}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,12,14,17	4,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,12,14,16,18	4,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,12,14,17,18	4,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,12,14,16	4,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,12	4,13	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,12,16,17,18	4,13,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,12,18	4,13,15,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,12,16,17	4,13,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,12,14,17,18	4,13,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,12,14,16	4,13	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,12,14,17	4,13,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,12,14,16,18	4,13,15,18	2^{-23}

Table 0.1154 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,17,18	4,11,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,16	4,11	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,17	4,11,15,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,16,18	4,11,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,14	4,11	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,14,16,17,18	4,11,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,14,18	4,11,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,14,16,17	4,11,15,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,17	4,11,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,16,18	4,11,13,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,17,18	4,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,16	4,11,13,15	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,14,18	4,11,13,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,14,16,17	4,11,13,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,14	4,11,13,15	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,14,16,17,18	4,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,12	4,11	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,12,16,17,18	4,11,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,12,18	4,11,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,12,16,17	4,11,15,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,12,14,17,18	4,11,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,12,14,16	4,11	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,12,14,17	4,11,15,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,12,14,16,18	4,11,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,12,18	4,11,13,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,12,16,17	4,11,13,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,12	4,11,13,15	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,12,16,17,18	4,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,12,14,17	4,11,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,12,14,16,18	4,11,13,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,12,14,17,18	4,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,12,14,16	4,11,13,15	2^{-12}

Table 0.1155 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,10,18	4,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,10,16,17	4,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,10	4,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,10,16,17,18	4,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,10,14,17	4,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,10,14,16,18	4,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,10,14,17,18	4,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,10,14,16	4,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,10	4,13	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,10,16,17,18	4,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,10,18	4,13,15,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,10,16,17	4,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,10,14,17,18	4,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,10,14,16	4,13	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,10,14,17	4,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,10,14,16,18	4,13,15,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,10,12,17	4,17	2^{-1}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,10,12,16,18	4,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,10,12,17,18	4,15,17,18	2^{-1}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,10,12,16	4,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,10,12,14,18	4,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,10,12,14,16,17	4,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,10,12,14	4,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,10,12,14,16,17,18	4,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,10,12,17,18	4,13,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,10,12,16	4,13	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,10,12,17	4,13,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,10,12,16,18	4,13,15,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,10,12,14	4,13	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,10,12,14,16,17,18	4,13,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,10,12,14,18	4,13,15,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,10,12,14,16,17	4,13,15,17	$2^{-6.5}$

Table 0.1156 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,10	4,11	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,10,16,17,18	4,11,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,10,18	4,11,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,10,16,17	4,11,15,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,10,14,17,18	4,11,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,10,14,16	4,11	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,10,14,17	4,11,15,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,10,14,16,18	4,11,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,10,18	4,11,13,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,10,16,17	4,11,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,10	4,11,13,15	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,10,16,17,18	4,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,10,14,17	4,11,13,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,10,14,16,18	4,11,13,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,10,14,17,18	4,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,10,14,16	4,11,13,15	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,10,12,17,18	4,11,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,10,12,16	4,11	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,10,12,17	4,11,15,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,10,12,16,18	4,11,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,10,12,14	4,11	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,10,12,14,16,17,18	4,11,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,10,12,14,18	4,11,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,10,12,14,16,17	4,11,15,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,10,12,17	4,11,13,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,10,12,16,18	4,11,13,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,10,12,17,18	4,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,10,12,16	4,11,13,15	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,10,12,14,18	4,11,13,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,10,12,14,16,17	4,11,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,10,12,14	4,11,13,15	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,10,12,14,16,17,18	4,11,13,15,17,18	$2^{-17.5}$

Table 0.1157 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,17,18	4,9,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,16	4,9	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,17	4,9,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,16,18	4,9,15,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,14	4,9	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,14,16,17,18	4,9,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,14,18	4,9,15,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,14,16,17	4,9,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,17	4,9,13,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,16,18	4,9,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,17,18	4,9,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,16	4,9,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,14,18	4,9,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,14,16,17	4,9,13,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,14	4,9,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,14,16,17,18	4,9,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,12	4,9	2^{-1}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,12,16,17,18	4,9,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,12,18	4,9,15,18	2^{-1}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,12,16,17	4,9,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,12,14,17,18	4,9,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,12,14,16	4,9	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,12,14,17	4,9,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,12,14,16,18	4,9,15,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,12,18	4,9,13,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,12,16,17	4,9,13,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,12	4,9,13,15	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,12,16,17,18	4,9,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,12,14,17	4,9,13,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,12,14,16,18	4,9,13,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,12,14,17,18	4,9,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,12,14,16	4,9,13,15	$2^{-6.5}$

Table 0.1158 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,17	4,9,11,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,16,18	4,9,11,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,17,18	4,9,11,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,16	4,9,11,15	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,14,18	4,9,11,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,14,16,17	4,9,11,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,14	4,9,11,15	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,14,16,17,18	4,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,17,18	4,9,11,13,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,16	4,9,11,13	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,17	4,9,11,13,15,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,16,18	4,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,14	4,9,11,13	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,14,16,17,18	4,9,11,13,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,14,18	4,9,11,13,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,14,16,17	4,9,11,13,15,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,12,18	4,9,11,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,12,16,17	4,9,11,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,12	4,9,11,15	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,12,16,17,18	4,9,11,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,12,14,17	4,9,11,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,12,14,16,18	4,9,11,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,12,14,17,18	4,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,12,14,16	4,9,11,15	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,12	4,9,11,13	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,12,16,17,18	4,9,11,13,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,12,18	4,9,11,13,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,12,16,17	4,9,11,13,15,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,12,14,17,18	4,9,11,13,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,12,14,16	4,9,11,13	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,12,14,17	4,9,11,13,15,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,12,14,16,18	4,9,11,13,15,18	$2^{-17.5}$

Table 0.1159 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,10	4,9	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,10,16,17,18	4,9,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,10,18	4,9,15,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,10,16,17	4,9,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,10,14,17,18	4,9,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,10,14,16	4,9	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,10,14,17	4,9,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,10,14,16,18	4,9,15,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,10,18	4,9,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,10,16,17	4,9,13,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,10	4,9,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,10,16,17,18	4,9,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,10,14,17	4,9,13,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,10,14,16,18	4,9,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,10,14,17,18	4,9,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,10,14,16	4,9,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,10,12,17,18	4,9,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,10,12,16	4,9	2^{-34}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,10,12,17	4,9,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,10,12,16,18	4,9,15,18	2^{-34}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,10,12,14	4,9	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,10,12,14,16,17,18	4,9,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,10,12,14,18	4,9,15,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,10,12,14,16,17	4,9,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,10,12,17	4,9,13,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,10,12,16,18	4,9,13,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,10,12,17,18	4,9,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,10,12,16	4,9,13,15	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,10,12,14,18	4,9,13,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,10,12,14,16,17	4,9,13,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,10,12,14	4,9,13,15	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,10,12,14,16,17,18	4,9,13,15,17,18	2^{-23}

Table 0.1160 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,10,18	4,9,11,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,10,16,17	4,9,11,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,10	4,9,11,15	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,10,16,17,18	4,9,11,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,10,14,17	4,9,11,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,10,14,16,18	4,9,11,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,10,14,17,18	4,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,10,14,16	4,9,11,15	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,10	4,9,11,13	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,10,16,17,18	4,9,11,13,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,10,18	4,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,10,16,17	4,9,11,13,15,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,10,14,17,18	4,9,11,13,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,10,14,16	4,9,11,13	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,10,14,17	4,9,11,13,15,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,10,14,16,18	4,9,11,13,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,10,12,17	4,9,11,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,10,12,16,18	4,9,11,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,10,12,17,18	4,9,11,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,10,12,16	4,9,11,15	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,10,12,14,18	4,9,11,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,10,12,14,16,17	4,9,11,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,10,12,14	4,9,11,15	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,10,12,14,16,17,18	4,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,10,12,17,18	4,9,11,13,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,10,12,16	4,9,11,13	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,10,12,17	4,9,11,13,15,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,10,12,16,18	4,9,11,13,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,10,12,14	4,9,11,13	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,10,12,14,16,17,18	4,9,11,13,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,10,12,14,18	4,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,10,12,14,16,17	4,9,11,13,15,17	2^{-12}

Table 0.1161 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,18	4,8,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,16,17	4,8,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1	4,8,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,16,17,18	4,8,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,14,17	4,8,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,14,16,18	4,8,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,14,17,18	4,8,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,14,16	4,8,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1	4,8,13	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,16,17,18	4,8,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,18	4,8,13,15,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,16,17	4,8,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,14,17,18	4,8,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,14,16	4,8,13	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,14,17	4,8,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,14,16,18	4,8,13,15,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,12,17	4,8,17	2^{-34}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,12,16,18	4,8,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,12,17,18	4,8,15,17,18	2^{-34}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,12,16	4,8,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,12,14,18	4,8,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,12,14,16,17	4,8,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,12,14	4,8,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,12,14,16,17,18	4,8,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,12,17,18	4,8,13,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,12,16	4,8,13	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,12,17	4,8,13,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,12,16,18	4,8,13,15,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,12,14	4,8,13	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,12,14,16,17,18	4,8,13,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,12,14,18	4,8,13,15,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,12,14,16,17	4,8,13,15,17	$2^{-28.5}$

Table 0.1162 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1	4,8,11	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,16,17,18	4,8,11,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,18	4,8,11,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,16,17	4,8,11,15,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,14,17,18	4,8,11,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,14,16	4,8,11	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,14,17	4,8,11,15,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,14,16,18	4,8,11,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,18	4,8,11,13,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,16,17	4,8,11,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1	4,8,11,13,15	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,16,17,18	4,8,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,14,17	4,8,11,13,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,14,16,18	4,8,11,13,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,14,17,18	4,8,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,14,16	4,8,11,13,15	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,12,17,18	4,8,11,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,12,16	4,8,11	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,12,17	4,8,11,15,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,12,16,18	4,8,11,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,12,14	4,8,11	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,12,14,16,17,18	4,8,11,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,12,14,18	4,8,11,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,12,14,16,17	4,8,11,15,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,12,17	4,8,11,13,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,12,16,18	4,8,11,13,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,12,17,18	4,8,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,12,16	4,8,11,13,15	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,12,14,18	4,8,11,13,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,12,14,16,17	4,8,11,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,12,14	4,8,11,13,15	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,12,14,16,17,18	4,8,11,13,15,17,18	$2^{-17.5}$

Table 0.1163 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(2)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,10,17	4,8,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,10,16,18	4,8,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,10,17,18	4,8,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,10,16	4,8,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,10,14,18	4,8,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,10,14,16,17	4,8,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,10,14	4,8,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,10,14,16,17,18	4,8,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,10,17,18	4,8,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,10,16	4,8,13	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,10,17	4,8,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,10,16,18	4,8,13,15,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,10,14	4,8,13	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,10,14,16,17,18	4,8,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,10,14,18	4,8,13,15,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,10,14,16,17	4,8,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,10,12,18	4,8,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,10,12,16,17	4,8,17	2^{-1}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,10,12	4,8,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,10,12,16,17,18	4,8,15,17,18	2^{-1}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,10,12,14,17	4,8,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,10,12,14,16,18	4,8,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,10,12,14,17,18	4,8,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,10,12,14,16	4,8,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,10,12	4,8,13	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,10,12,16,17,18	4,8,13,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,10,12,18	4,8,13,15,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,10,12,16,17	4,8,13,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,10,12,14,17,18	4,8,13,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,10,12,14,16	4,8,13	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,10,12,14,17	4,8,13,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,10,12,14,16,18	4,8,13,15,18	2^{-12}

Table 0.1164 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,10,17,18	4,8,11,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,10,16	4,8,11	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,10,17	4,8,11,15,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,10,16,18	4,8,11,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,10,14	4,8,11	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,10,14,16,17,18	4,8,11,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,10,14,18	4,8,11,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,10,14,16,17	4,8,11,15,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,10,17	4,8,11,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,10,16,18	4,8,11,13,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,10,17,18	4,8,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,10,16	4,8,11,13,15	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,10,14,18	4,8,11,13,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,10,14,16,17	4,8,11,13,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,10,14	4,8,11,13,15	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,10,14,16,17,18	4,8,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,10,12	4,8,11	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,10,12,16,17,18	4,8,11,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,10,12,18	4,8,11,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,10,12,16,17	4,8,11,15,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,10,12,14,17,18	4,8,11,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,10,12,14,16	4,8,11	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,10,12,14,17	4,8,11,15,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,10,12,14,16,18	4,8,11,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,10,12,18	4,8,11,13,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,10,12,16,17	4,8,11,13,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,10,12	4,8,11,13,15	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,10,12,16,17,18	4,8,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,10,12,14,17	4,8,11,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,10,12,14,16,18	4,8,11,13,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,10,12,14,17,18	4,8,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,10,12,14,16	4,8,11,13,15	2^{-23}

Table 0.1165 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1	4,8,9	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,16,17,18	4,8,9,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,18	4,8,9,15,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,16,17	4,8,9,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,14,17,18	4,8,9,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,14,16	4,8,9	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,14,17	4,8,9,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,14,16,18	4,8,9,15,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,18	4,8,9,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,16,17	4,8,9,13,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1	4,8,9,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,16,17,18	4,8,9,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,14,17	4,8,9,13,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,14,16,18	4,8,9,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,14,17,18	4,8,9,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,14,16	4,8,9,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,12,17,18	4,8,9,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,12,16	4,8,9	2^{-1}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,12,17	4,8,9,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,12,16,18	4,8,9,15,18	2^{-1}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,12,14	4,8,9	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,12,14,16,17,18	4,8,9,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,12,14,18	4,8,9,15,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,12,14,16,17	4,8,9,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,12,17	4,8,9,13,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,12,16,18	4,8,9,13,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,12,17,18	4,8,9,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,12,16	4,8,9,13,15	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,12,14,18	4,8,9,13,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,12,14,16,17	4,8,9,13,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,12,14	4,8,9,13,15	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,12,14,16,17,18	4,8,9,13,15,17,18	2^{-12}

Table 0.1166 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,18	4,8,9,11,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,16,17	4,8,9,11,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1	4,8,9,11,15	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,16,17,18	4,8,9,11,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,14,17	4,8,9,11,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,14,16,18	4,8,9,11,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,14,17,18	4,8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,14,16	4,8,9,11,15	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1	4,8,9,11,13	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,16,17,18	4,8,9,11,13,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,18	4,8,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,16,17	4,8,9,11,13,15,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,14,17,18	4,8,9,11,13,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,14,16	4,8,9,11,13	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,14,17	4,8,9,11,13,15,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,14,16,18	4,8,9,11,13,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,12,17	4,8,9,11,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,12,16,18	4,8,9,11,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,12,17,18	4,8,9,11,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,12,16	4,8,9,11,15	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,12,14,18	4,8,9,11,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,12,14,16,17	4,8,9,11,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,12,14	4,8,9,11,15	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,12,14,16,17,18	4,8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,12,17,18	4,8,9,11,13,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,12,16	4,8,9,11,13	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,12,17	4,8,9,11,13,15,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,12,16,18	4,8,9,11,13,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,12,14	4,8,9,11,13	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,12,14,16,17,18	4,8,9,11,13,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,12,14,18	4,8,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,12,14,16,17	4,8,9,11,13,15,17	2^{-23}

Table 0.1167 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,10,17,18	4,8,9,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,10,16	4,8,9	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,10,17	4,8,9,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,10,16,18	4,8,9,15,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,10,14	4,8,9	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,10,14,16,17,18	4,8,9,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,10,14,18	4,8,9,15,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,10,14,16,17	4,8,9,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,10,17	4,8,9,13,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,10,16,18	4,8,9,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,10,17,18	4,8,9,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,10,16	4,8,9,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,10,14,18	4,8,9,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,10,14,16,17	4,8,9,13,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,10,14	4,8,9,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,10,14,16,17,18	4,8,9,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,10,12	4,8,9	2^{-34}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,10,12,16,17,18	4,8,9,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,10,12,18	4,8,9,15,18	2^{-34}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,10,12,16,17	4,8,9,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,10,12,14,17,18	4,8,9,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,10,12,14,16	4,8,9	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,10,12,14,17	4,8,9,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,10,12,14,16,18	4,8,9,15,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,10,12,18	4,8,9,13,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,10,12,16,17	4,8,9,13,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,10,12	4,8,9,13,15	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,10,12,16,17,18	4,8,9,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,10,12,14,17	4,8,9,13,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,10,12,14,16,18	4,8,9,13,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,10,12,14,17,18	4,8,9,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,10,12,14,16	4,8,9,13,15	$2^{-28.5}$

Table 0.1168 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,10,17	4,8,9,11,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,10,16,18	4,8,9,11,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,10,17,18	4,8,9,11,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,10,16	4,8,9,11,15	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,10,14,18	4,8,9,11,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,10,14,16,17	4,8,9,11,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,10,14	4,8,9,11,15	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,10,14,16,17,18	4,8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,10,17,18	4,8,9,11,13,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,10,16	4,8,9,11,13	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,10,17	4,8,9,11,13,15,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,10,16,18	4,8,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,10,14	4,8,9,11,13	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,10,14,16,17,18	4,8,9,11,13,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,10,14,18	4,8,9,11,13,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,10,14,16,17	4,8,9,11,13,15,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,10,12,18	4,8,9,11,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,10,12,16,17	4,8,9,11,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,10,12	4,8,9,11,15	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,10,12,16,17,18	4,8,9,11,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,10,12,14,17	4,8,9,11,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,10,12,14,16,18	4,8,9,11,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,10,12,14,17,18	4,8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,10,12,14,16	4,8,9,11,15	2^{-23}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,10,12	4,8,9,11,13	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,10,12,16,17,18	4,8,9,11,13,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,10,12,18	4,8,9,11,13,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,10,12,16,17	4,8,9,11,13,15,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,10,12,14,17,18	4,8,9,11,13,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,10,12,14,16	4,8,9,11,13	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,10,12,14,17	4,8,9,11,13,15,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,10,12,14,16,18	4,8,9,11,13,15,18	$2^{-17.5}$

Table 0.1169 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,7,17,18	4,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,7,16	4	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,7,17	4,15,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,7,16,18	4,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,7,14	4	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,7,14,16,17,18	4,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,7,14,18	4,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,7,14,16,17	4,15,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,7,17	4,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,7,16,18	4,13,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,7,17,18	4,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,7,16	4,13,15	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,7,14,18	4,13,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,7,14,16,17	4,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,7,14	4,13,15	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,7,14,16,17,18	4,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,7,12	4	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,7,12,16,17,18	4,17,18	2^{-34}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,7,12,18	4,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,7,12,16,17	4,15,17	2^{-34}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,7,12,14,17,18	4,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,7,12,14,16	4	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,7,12,14,17	4,15,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,7,12,14,16,18	4,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,7,12,18	4,13,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,7,12,16,17	4,13,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,7,12	4,13,15	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,7,12,16,17,18	4,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,7,12,14,17	4,13,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,7,12,14,16,18	4,13,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,7,12,14,17,18	4,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,7,12,14,16	4,13,15	2^{-23}

Table 0.1170 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,7,17	4,11,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,7,16,18	4,11,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,7,17,18	4,11,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,7,16	4,11,15	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,7,14,18	4,11,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,7,14,16,17	4,11,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,7,14	4,11,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,7,14,16,17,18	4,11,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,7,17,18	4,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,7,16	4,11,13	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,7,17	4,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,7,16,18	4,11,13,15,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,7,14	4,11,13	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,7,14,16,17,18	4,11,13,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,7,14,18	4,11,13,15,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,7,14,16,17	4,11,13,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,7,12,18	4,11,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,7,12,16,17	4,11,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,7,12	4,11,15	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,7,12,16,17,18	4,11,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,7,12,14,17	4,11,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,7,12,14,16,18	4,11,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,7,12,14,17,18	4,11,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,7,12,14,16	4,11,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,7,12	4,11,13	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,7,12,16,17,18	4,11,13,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,7,12,18	4,11,13,15,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,7,12,16,17	4,11,13,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,7,12,14,17,18	4,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,7,12,14,16	4,11,13	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,7,12,14,17	4,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,7,12,14,16,18	4,11,13,15,18	2^{-12}

Table 0.1171 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,7,10	4	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,7,10,16,17,18	4,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,7,10,18	4,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,7,10,16,17	4,15,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,7,10,14,17,18	4,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,7,10,14,16	4	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,7,10,14,17	4,15,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,7,10,14,16,18	4,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,7,10,18	4,13,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,7,10,16,17	4,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,7,10	4,13,15	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,7,10,16,17,18	4,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,7,10,14,17	4,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,7,10,14,16,18	4,13,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,7,10,14,17,18	4,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,7,10,14,16	4,13,15	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,7,10,12,17,18	4,17,18	2^{-1}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,7,10,12,16	4	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,7,10,12,17	4,15,17	2^{-1}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,7,10,12,16,18	4,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,7,10,12,14	4	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,7,10,12,14,16,17,18	4,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,7,10,12,14,18	4,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,7,10,12,14,16,17	4,15,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,7,10,12,17	4,13,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,7,10,12,16,18	4,13,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,7,10,12,17,18	4,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,7,10,12,16	4,13,15	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,7,10,12,14,18	4,13,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,7,10,12,14,16,17	4,13,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,7,10,12,14	4,13,15	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,7,10,12,14,16,17,18	4,13,15,17,18	$2^{-6.5}$

Table 0.1172 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,7,10,18	4,11,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,7,10,16,17	4,11,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,7,10	4,11,15	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,7,10,16,17,18	4,11,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,7,10,14,17	4,11,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,7,10,14,16,18	4,11,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,7,10,14,17,18	4,11,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,7,10,14,16	4,11,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,7,10	4,11,13	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,7,10,16,17,18	4,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,7,10,18	4,11,13,15,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,7,10,16,17	4,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,7,10,14,17,18	4,11,13,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,7,10,14,16	4,11,13	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,7,10,14,17	4,11,13,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,7,10,14,16,18	4,11,13,15,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,7,10,12,17	4,11,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,7,10,12,16,18	4,11,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,7,10,12,17,18	4,11,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,7,10,12,16	4,11,15	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,7,10,12,14,18	4,11,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,7,10,12,14,16,17	4,11,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,7,10,12,14	4,11,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,7,10,12,14,16,17,18	4,11,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,7,10,12,17,18	4,11,13,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,7,10,12,16	4,11,13	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,7,10,12,17	4,11,13,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,7,10,12,16,18	4,11,13,15,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,7,10,12,14	4,11,13	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,7,10,12,14,16,17,18	4,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,7,10,12,14,18	4,11,13,15,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,7,10,12,14,16,17	4,11,13,15,17	$2^{-17.5}$

Table 0.1173 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,7,17	4,9,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,7,16,18	4,9,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,7,17,18	4,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,7,16	4,9,15	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,7,14,18	4,9,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,7,14,16,17	4,9,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,7,14	4,9,15	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,7,14,16,17,18	4,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,7,17,18	4,9,13,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,7,16	4,9,13	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,7,17	4,9,13,15,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,7,16,18	4,9,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,7,14	4,9,13	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,7,14,16,17,18	4,9,13,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,7,14,18	4,9,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,7,14,16,17	4,9,13,15,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,7,12,18	4,9,18	2^{-1}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,7,12,16,17	4,9,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,7,12	4,9,15	2^{-1}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,7,12,16,17,18	4,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,7,12,14,17	4,9,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,7,12,14,16,18	4,9,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,7,12,14,17,18	4,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,7,12,14,16	4,9,15	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,7,12	4,9,13	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,7,12,16,17,18	4,9,13,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,7,12,18	4,9,13,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,7,12,16,17	4,9,13,15,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,7,12,14,17,18	4,9,13,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,7,12,14,16	4,9,13	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,7,12,14,17	4,9,13,15,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,7,12,14,16,18	4,9,13,15,18	$2^{-6.5}$

Table 0.1174 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,7,17,18	4,9,11,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,7,16	4,9,11	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,7,17	4,9,11,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,7,16,18	4,9,11,15,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,7,14	4,9,11	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,7,14,16,17,18	4,9,11,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,7,14,18	4,9,11,15,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,7,14,16,17	4,9,11,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,7,17	4,9,11,13,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,7,16,18	4,9,11,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,7,17,18	4,9,11,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,7,16	4,9,11,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,7,14,18	4,9,11,13,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,7,14,16,17	4,9,11,13,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,7,14	4,9,11,13,15	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,7,14,16,17,18	4,9,11,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,7,12	4,9,11	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,7,12,16,17,18	4,9,11,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,7,12,18	4,9,11,15,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,7,12,16,17	4,9,11,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,7,12,14,17,18	4,9,11,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,7,12,14,16	4,9,11	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,7,12,14,17	4,9,11,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,7,12,14,16,18	4,9,11,15,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,7,12,18	4,9,11,13,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,7,12,16,17	4,9,11,13,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,7,12	4,9,11,13,15	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,7,12,16,17,18	4,9,11,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,7,12,14,17	4,9,11,13,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,7,12,14,16,18	4,9,11,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,7,12,14,17,18	4,9,11,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,7,12,14,16	4,9,11,13,15	$2^{-17.5}$

Table 0.1175 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,7,10,18	4,9,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,7,10,16,17	4,9,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,7,10	4,9,15	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,7,10,16,17,18	4,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,7,10,14,17	4,9,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,7,10,14,16,18	4,9,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,7,10,14,17,18	4,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,7,10,14,16	4,9,15	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,7,10	4,9,13	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,7,10,16,17,18	4,9,13,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,7,10,18	4,9,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,7,10,16,17	4,9,13,15,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,7,10,14,17,18	4,9,13,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,7,10,14,16	4,9,13	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,7,10,14,17	4,9,13,15,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,7,10,14,16,18	4,9,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,7,10,12,17	4,9,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,7,10,12,16,18	4,9,18	2^{-34}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,7,10,12,17,18	4,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,7,10,12,16	4,9,15	2^{-34}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,7,10,12,14,18	4,9,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,7,10,12,14,16,17	4,9,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,7,10,12,14	4,9,15	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,7,10,12,14,16,17,18	4,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,7,10,12,17,18	4,9,13,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,7,10,12,16	4,9,13	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,7,10,12,17	4,9,13,15,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,7,10,12,16,18	4,9,13,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,7,10,12,14	4,9,13	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,7,10,12,14,16,17,18	4,9,13,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,7,10,12,14,18	4,9,13,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,7,10,12,14,16,17	4,9,13,15,17	2^{-23}

Table 0.1176 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,7,10	4,9,11	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,7,10,16,17,18	4,9,11,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,7,10,18	4,9,11,15,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,7,10,16,17	4,9,11,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,7,10,14,17,18	4,9,11,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,7,10,14,16	4,9,11	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,7,10,14,17	4,9,11,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,7,10,14,16,18	4,9,11,15,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,7,10,18	4,9,11,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,7,10,16,17	4,9,11,13,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,7,10	4,9,11,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,7,10,16,17,18	4,9,11,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,7,10,14,17	4,9,11,13,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,7,10,14,16,18	4,9,11,13,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,7,10,14,17,18	4,9,11,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,7,10,14,16	4,9,11,13,15	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,7,10,12,17,18	4,9,11,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,7,10,12,16	4,9,11	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,7,10,12,17	4,9,11,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,7,10,12,16,18	4,9,11,15,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,7,10,12,14	4,9,11	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,7,10,12,14,16,17,18	4,9,11,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,7,10,12,14,18	4,9,11,15,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,7,10,12,14,16,17	4,9,11,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,7,10,12,17	4,9,11,13,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,7,10,12,16,18	4,9,11,13,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,7,10,12,17,18	4,9,11,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,7,10,12,16	4,9,11,13,15	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,7,10,12,14,18	4,9,11,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,7,10,12,14,16,17	4,9,11,13,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,7,10,12,14	4,9,11,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,7,10,12,14,16,17,18	4,9,11,13,15,17,18	2^{-12}

Table 0.1177 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,7	4,8	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,7,16,17,18	4,8,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,7,18	4,8,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,7,16,17	4,8,15,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,7,14,17,18	4,8,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,7,14,16	4,8	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,7,14,17	4,8,15,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,7,14,16,18	4,8,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,7,18	4,8,13,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,7,16,17	4,8,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,7	4,8,13,15	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,7,16,17,18	4,8,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,7,14,17	4,8,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,7,14,16,18	4,8,13,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,7,14,17,18	4,8,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,7,14,16	4,8,13,15	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,7,12,17,18	4,8,17,18	2^{-34}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,7,12,16	4,8	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,7,12,17	4,8,15,17	2^{-34}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,7,12,16,18	4,8,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,7,12,14	4,8	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,7,12,14,16,17,18	4,8,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,7,12,14,18	4,8,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,7,12,14,16,17	4,8,15,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,7,12,17	4,8,13,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,7,12,16,18	4,8,13,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,7,12,17,18	4,8,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,7,12,16	4,8,13,15	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,7,12,14,18	4,8,13,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,7,12,14,16,17	4,8,13,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,7,12,14	4,8,13,15	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,7,12,14,16,17,18	4,8,13,15,17,18	$2^{-28.5}$

Table 0.1178 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,7,18	4,8,11,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,7,16,17	4,8,11,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,7	4,8,11,15	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,7,16,17,18	4,8,11,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,7,14,17	4,8,11,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,7,14,16,18	4,8,11,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,7,14,17,18	4,8,11,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,7,14,16	4,8,11,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,7	4,8,11,13	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,7,16,17,18	4,8,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,7,18	4,8,11,13,15,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,7,16,17	4,8,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,7,14,17,18	4,8,11,13,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,7,14,16	4,8,11,13	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,7,14,17	4,8,11,13,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,7,14,16,18	4,8,11,13,15,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,7,12,17	4,8,11,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,7,12,16,18	4,8,11,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,7,12,17,18	4,8,11,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,7,12,16	4,8,11,15	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,7,12,14,18	4,8,11,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,7,12,14,16,17	4,8,11,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,7,12,14	4,8,11,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,7,12,14,16,17,18	4,8,11,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,7,12,17,18	4,8,11,13,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,7,12,16	4,8,11,13	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,7,12,17	4,8,11,13,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,7,12,16,18	4,8,11,13,15,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,7,12,14	4,8,11,13	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,7,12,14,16,17,18	4,8,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,7,12,14,18	4,8,11,13,15,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,7,12,14,16,17	4,8,11,13,15,17	$2^{-17.5}$

Table 0.1179 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,7,10,17,18	4,8,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,7,10,16	4,8	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,7,10,17	4,8,15,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,7,10,16,18	4,8,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,7,10,14	4,8	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,7,10,14,16,17,18	4,8,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,7,10,14,18	4,8,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,7,10,14,16,17	4,8,15,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,7,10,17	4,8,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,7,10,16,18	4,8,13,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,7,10,17,18	4,8,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,7,10,16	4,8,13,15	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,7,10,14,18	4,8,13,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,7,10,14,16,17	4,8,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,7,10,14	4,8,13,15	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,7,10,14,16,17,18	4,8,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,7,10,12	4,8	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,7,10,12,16,17,18	4,8,17,18	2^{-1}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,7,10,12,18	4,8,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,7,10,12,16,17	4,8,15,17	2^{-1}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,7,10,12,14,17,18	4,8,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,7,10,12,14,16	4,8	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,7,10,12,14,17	4,8,15,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,7,10,12,14,16,18	4,8,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,7,10,12,18	4,8,13,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,7,10,12,16,17	4,8,13,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,7,10,12	4,8,13,15	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,7,10,12,16,17,18	4,8,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,7,10,12,14,17	4,8,13,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,7,10,12,14,16,18	4,8,13,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,7,10,12,14,17,18	4,8,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,7,10,12,14,16	4,8,13,15	2^{-12}

Table 0.1180 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,7,10,17	4,8,11,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,7,10,16,18	4,8,11,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,7,10,17,18	4,8,11,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,7,10,16	4,8,11,15	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,7,10,14,18	4,8,11,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,7,10,14,16,17	4,8,11,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,7,10,14	4,8,11,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,7,10,14,16,17,18	4,8,11,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,7,10,17,18	4,8,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,7,10,16	4,8,11,13	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,7,10,17	4,8,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,7,10,16,18	4,8,11,13,15,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,7,10,14	4,8,11,13	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,7,10,14,16,17,18	4,8,11,13,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,7,10,14,18	4,8,11,13,15,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,7,10,14,16,17	4,8,11,13,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,7,10,12,18	4,8,11,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,7,10,12,16,17	4,8,11,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,7,10,12	4,8,11,15	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,7,10,12,16,17,18	4,8,11,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,7,10,12,14,17	4,8,11,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,7,10,12,14,16,18	4,8,11,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,7,10,12,14,17,18	4,8,11,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,7,10,12,14,16	4,8,11,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,7,10,12	4,8,11,13	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,7,10,12,16,17,18	4,8,11,13,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,7,10,12,18	4,8,11,13,15,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,7,10,12,16,17	4,8,11,13,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,7,10,12,14,17,18	4,8,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,7,10,12,14,16	4,8,11,13	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,7,10,12,14,17	4,8,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,7,10,12,14,16,18	4,8,11,13,15,18	2^{-23}

Table 0.1181 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,7,18	4,8,9,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,7,16,17	4,8,9,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,7	4,8,9,15	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,7,16,17,18	4,8,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,7,14,17	4,8,9,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,7,14,16,18	4,8,9,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,7,14,17,18	4,8,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,7,14,16	4,8,9,15	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,7	4,8,9,13	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,7,16,17,18	4,8,9,13,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,7,18	4,8,9,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,7,16,17	4,8,9,13,15,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,7,14,17,18	4,8,9,13,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,7,14,16	4,8,9,13	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,7,14,17	4,8,9,13,15,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,7,14,16,18	4,8,9,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,7,12,17	4,8,9,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,7,12,16,18	4,8,9,18	2^{-1}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,7,12,17,18	4,8,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,7,12,16	4,8,9,15	2^{-1}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,7,12,14,18	4,8,9,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,7,12,14,16,17	4,8,9,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,7,12,14	4,8,9,15	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,7,12,14,16,17,18	4,8,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,7,12,17,18	4,8,9,13,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,7,12,16	4,8,9,13	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,7,12,17	4,8,9,13,15,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,7,12,16,18	4,8,9,13,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,7,12,14	4,8,9,13	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,7,12,14,16,17,18	4,8,9,13,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,7,12,14,18	4,8,9,13,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,7,12,14,16,17	4,8,9,13,15,17	2^{-12}

Table 0.1182 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,7	4,8,9,11	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,7,16,17,18	4,8,9,11,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,7,18	4,8,9,11,15,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,7,16,17	4,8,9,11,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,7,14,17,18	4,8,9,11,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,7,14,16	4,8,9,11	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,7,14,17	4,8,9,11,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,7,14,16,18	4,8,9,11,15,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,7,18	4,8,9,11,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,7,16,17	4,8,9,11,13,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,7	4,8,9,11,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,7,16,17,18	4,8,9,11,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,7,14,17	4,8,9,11,13,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,7,14,16,18	4,8,9,11,13,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,7,14,17,18	4,8,9,11,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,7,14,16	4,8,9,11,13,15	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,7,12,17,18	4,8,9,11,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,7,12,16	4,8,9,11	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,7,12,17	4,8,9,11,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,7,12,16,18	4,8,9,11,15,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,7,12,14	4,8,9,11	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,7,12,14,16,17,18	4,8,9,11,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,7,12,14,18	4,8,9,11,15,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,7,12,14,16,17	4,8,9,11,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,7,12,17	4,8,9,11,13,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,7,12,16,18	4,8,9,11,13,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,7,12,17,18	4,8,9,11,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,7,12,16	4,8,9,11,13,15	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,7,12,14,18	4,8,9,11,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,7,12,14,16,17	4,8,9,11,13,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,7,12,14	4,8,9,11,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,7,12,14,16,17,18	4,8,9,11,13,15,17,18	2^{-23}

Table 0.1183 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,7,10,17	4,8,9,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,7,10,16,18	4,8,9,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,7,10,17,18	4,8,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,7,10,16	4,8,9,15	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,7,10,14,18	4,8,9,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,7,10,14,16,17	4,8,9,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,7,10,14	4,8,9,15	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,7,10,14,16,17,18	4,8,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,7,10,17,18	4,8,9,13,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,7,10,16	4,8,9,13	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,7,10,17	4,8,9,13,15,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,7,10,16,18	4,8,9,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,7,10,14	4,8,9,13	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,7,10,14,16,17,18	4,8,9,13,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,7,10,14,18	4,8,9,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,7,10,14,16,17	4,8,9,13,15,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,7,10,12,18	4,8,9,18	2^{-34}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,7,10,12,16,17	4,8,9,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,7,10,12	4,8,9,15	2^{-34}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,7,10,12,16,17,18	4,8,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,7,10,12,14,17	4,8,9,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,7,10,12,14,16,18	4,8,9,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,7,10,12,14,17,18	4,8,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,7,10,12,14,16	4,8,9,15	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,7,10,12	4,8,9,13	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,7,10,12,16,17,18	4,8,9,13,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,7,10,12,18	4,8,9,13,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,7,10,12,16,17	4,8,9,13,15,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,7,10,12,14,17,18	4,8,9,13,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,7,10,12,14,16	4,8,9,13	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,7,10,12,14,17	4,8,9,13,15,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,7,10,12,14,16,18	4,8,9,13,15,18	$2^{-28.5}$

Table 0.1184 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,7,10,17,18	4,8,9,11,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,7,10,16	4,8,9,11	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,7,10,17	4,8,9,11,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,7,10,16,18	4,8,9,11,15,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,7,10,14	4,8,9,11	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,7,10,14,16,17,18	4,8,9,11,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,7,10,14,18	4,8,9,11,15,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,7,10,14,16,17	4,8,9,11,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,7,10,17	4,8,9,11,13,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,7,10,16,18	4,8,9,11,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,7,10,17,18	4,8,9,11,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,7,10,16	4,8,9,11,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,7,10,14,18	4,8,9,11,13,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,7,10,14,16,17	4,8,9,11,13,17	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,7,10,14	4,8,9,11,13,15	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,7,10,14,16,17,18	4,8,9,11,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,7,10,12	4,8,9,11	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,7,10,12,16,17,18	4,8,9,11,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,7,10,12,18	4,8,9,11,15,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,7,10,12,16,17	4,8,9,11,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,7,10,12,14,17,18	4,8,9,11,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,7,10,12,14,16	4,8,9,11	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,7,10,12,14,17	4,8,9,11,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,7,10,12,14,16,18	4,8,9,11,15,18	2^{-23}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,7,10,12,18	4,8,9,11,13,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,7,10,12,16,17	4,8,9,11,13,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,7,10,12	4,8,9,11,13,15	$2^{-28.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,7,10,12,16,17,18	4,8,9,11,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,7,10,12,14,17	4,8,9,11,13,17	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,7,10,12,14,16,18	4,8,9,11,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,7,10,12,14,17,18	4,8,9,11,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,7,10,12,14,16	4,8,9,11,13,15	$2^{-17.5}$

Table 0.1185 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,18	4,6,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,16,17	4,6,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1	4,6,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,16,17,18	4,6,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,14,17	4,6,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,14,16,18	4,6,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,14,17,18	4,6,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,14,16	4,6,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1	4,6,13	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,16,17,18	4,6,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,18	4,6,13,15,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,16,17	4,6,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,14,17,18	4,6,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,14,16	4,6,13	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,14,17	4,6,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,14,16,18	4,6,13,15,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,12,17	4,6,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,12,16,18	4,6,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,12,17,18	4,6,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,12,16	4,6,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,12,14,18	4,6,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,12,14,16,17	4,6,17	2^{-34}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,12,14	4,6,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,12,14,16,17,18	4,6,15,17,18	2^{-34}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,12,17,18	4,6,13,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,12,16	4,6,13	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,12,17	4,6,13,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,12,16,18	4,6,13,15,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,12,14	4,6,13	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,12,14,16,17,18	4,6,13,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,12,14,18	4,6,13,15,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,12,14,16,17	4,6,13,15,17	$2^{-28.5}$

Table 0.1186 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1	4,6,11	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,16,17,18	4,6,11,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,18	4,6,11,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,16,17	4,6,11,15,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,14,17,18	4,6,11,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,14,16	4,6,11	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,14,17	4,6,11,15,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,14,16,18	4,6,11,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,18	4,6,11,13,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,16,17	4,6,11,13,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1	4,6,11,13,15	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,16,17,18	4,6,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,14,17	4,6,11,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,14,16,18	4,6,11,13,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,14,17,18	4,6,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,14,16	4,6,11,13,15	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,12,17,18	4,6,11,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,12,16	4,6,11	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,12,17	4,6,11,15,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,12,16,18	4,6,11,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,12,14	4,6,11	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,12,14,16,17,18	4,6,11,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,12,14,18	4,6,11,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,12,14,16,17	4,6,11,15,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,12,17	4,6,11,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,12,16,18	4,6,11,13,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,12,17,18	4,6,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,12,16	4,6,11,13,15	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,12,14,18	4,6,11,13,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,12,14,16,17	4,6,11,13,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,12,14	4,6,11,13,15	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,12,14,16,17,18	4,6,11,13,15,17,18	$2^{-28.5}$

Table 0.1187 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(2)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,10,17	4,6,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,10,16,18	4,6,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,10,17,18	4,6,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,10,16	4,6,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,10,14,18	4,6,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,10,14,16,17	4,6,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,10,14	4,6,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,10,14,16,17,18	4,6,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,10,17,18	4,6,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,10,16	4,6,13	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,10,17	4,6,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,10,16,18	4,6,13,15,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,10,14	4,6,13	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,10,14,16,17,18	4,6,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,10,14,18	4,6,13,15,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,10,14,16,17	4,6,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,10,12,18	4,6,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,10,12,16,17	4,6,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,10,12	4,6,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,10,12,16,17,18	4,6,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,10,12,14,17	4,6,17	2^{-1}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,10,12,14,16,18	4,6,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,10,12,14,17,18	4,6,15,17,18	2^{-1}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,10,12,14,16	4,6,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,10,12	4,6,13	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,10,12,16,17,18	4,6,13,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,10,12,18	4,6,13,15,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,10,12,16,17	4,6,13,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,10,12,14,17,18	4,6,13,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,10,12,14,16	4,6,13	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,10,12,14,17	4,6,13,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,10,12,14,16,18	4,6,13,15,18	2^{-23}

Table 0.1188 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,10,17,18	4,6,11,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,10,16	4,6,11	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,10,17	4,6,11,15,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,10,16,18	4,6,11,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,10,14	4,6,11	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,10,14,16,17,18	4,6,11,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,10,14,18	4,6,11,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,10,14,16,17	4,6,11,15,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,10,17	4,6,11,13,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,10,16,18	4,6,11,13,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,10,17,18	4,6,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,10,16	4,6,11,13,15	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,10,14,18	4,6,11,13,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,10,14,16,17	4,6,11,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,10,14	4,6,11,13,15	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,10,14,16,17,18	4,6,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,10,12	4,6,11	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,10,12,16,17,18	4,6,11,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,10,12,18	4,6,11,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,10,12,16,17	4,6,11,15,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,10,12,14,17,18	4,6,11,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,10,12,14,16	4,6,11	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,10,12,14,17	4,6,11,15,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,10,12,14,16,18	4,6,11,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,10,12,18	4,6,11,13,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,10,12,16,17	4,6,11,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,10,12	4,6,11,13,15	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,10,12,16,17,18	4,6,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,10,12,14,17	4,6,11,13,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,10,12,14,16,18	4,6,11,13,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,10,12,14,17,18	4,6,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,10,12,14,16	4,6,11,13,15	2^{-23}

Table 0.1189 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1	4,6,9	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,16,17,18	4,6,9,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,18	4,6,9,15,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,16,17	4,6,9,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,14,17,18	4,6,9,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,14,16	4,6,9	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,14,17	4,6,9,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,14,16,18	4,6,9,15,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,18	4,6,9,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,16,17	4,6,9,13,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1	4,6,9,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,16,17,18	4,6,9,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,14,17	4,6,9,13,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,14,16,18	4,6,9,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,14,17,18	4,6,9,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,14,16	4,6,9,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,12,17,18	4,6,9,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,12,16	4,6,9	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,12,17	4,6,9,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,12,16,18	4,6,9,15,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,12,14	4,6,9	2^{-1}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,12,14,16,17,18	4,6,9,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,12,14,18	4,6,9,15,18	2^{-1}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,12,14,16,17	4,6,9,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,12,17	4,6,9,13,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,12,16,18	4,6,9,13,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,12,17,18	4,6,9,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,12,16	4,6,9,13,15	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,12,14,18	4,6,9,13,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,12,14,16,17	4,6,9,13,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,12,14	4,6,9,13,15	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,12,14,16,17,18	4,6,9,13,15,17,18	2^{-23}

Table 0.1190 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,18	4,6,9,11,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,16,17	4,6,9,11,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1	4,6,9,11,15	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,16,17,18	4,6,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,14,17	4,6,9,11,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,14,16,18	4,6,9,11,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,14,17,18	4,6,9,11,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,14,16	4,6,9,11,15	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1	4,6,9,11,13	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,16,17,18	4,6,9,11,13,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,18	4,6,9,11,13,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,16,17	4,6,9,11,13,15,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,14,17,18	4,6,9,11,13,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,14,16	4,6,9,11,13	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,14,17	4,6,9,11,13,15,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,14,16,18	4,6,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,12,17	4,6,9,11,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,12,16,18	4,6,9,11,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,12,17,18	4,6,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,12,16	4,6,9,11,15	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,12,14,18	4,6,9,11,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,12,14,16,17	4,6,9,11,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,12,14	4,6,9,11,15	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,12,14,16,17,18	4,6,9,11,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,12,17,18	4,6,9,11,13,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,12,16	4,6,9,11,13	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,12,17	4,6,9,11,13,15,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,12,16,18	4,6,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,12,14	4,6,9,11,13	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,12,14,16,17,18	4,6,9,11,13,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,12,14,18	4,6,9,11,13,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,12,14,16,17	4,6,9,11,13,15,17	2^{-23}

Table 0.1191 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,10,17,18	4,6,9,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,10,16	4,6,9	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,10,17	4,6,9,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,10,16,18	4,6,9,15,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,10,14	4,6,9	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,10,14,16,17,18	4,6,9,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,10,14,18	4,6,9,15,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,10,14,16,17	4,6,9,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,10,17	4,6,9,13,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,10,16,18	4,6,9,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,10,17,18	4,6,9,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,10,16	4,6,9,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,10,14,18	4,6,9,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,10,14,16,17	4,6,9,13,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,10,14	4,6,9,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,10,14,16,17,18	4,6,9,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,10,12	4,6,9	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,10,12,16,17,18	4,6,9,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,10,12,18	4,6,9,15,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,10,12,16,17	4,6,9,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,10,12,14,17,18	4,6,9,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,10,12,14,16	4,6,9	2^{-34}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,10,12,14,17	4,6,9,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,10,12,14,16,18	4,6,9,15,18	2^{-34}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,10,12,18	4,6,9,13,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,10,12,16,17	4,6,9,13,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,10,12	4,6,9,13,15	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,10,12,16,17,18	4,6,9,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,10,12,14,17	4,6,9,13,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,10,12,14,16,18	4,6,9,13,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,10,12,14,17,18	4,6,9,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,10,12,14,16	4,6,9,13,15	$2^{-28.5}$

Table 0.1192 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,10,17	4,6,9,11,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,10,16,18	4,6,9,11,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,10,17,18	4,6,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,10,16	4,6,9,11,15	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,10,14,18	4,6,9,11,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,10,14,16,17	4,6,9,11,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,10,14	4,6,9,11,15	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,10,14,16,17,18	4,6,9,11,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,10,17,18	4,6,9,11,13,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,10,16	4,6,9,11,13	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,10,17	4,6,9,11,13,15,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,10,16,18	4,6,9,11,13,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,10,14	4,6,9,11,13	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,10,14,16,17,18	4,6,9,11,13,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,10,14,18	4,6,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,10,14,16,17	4,6,9,11,13,15,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,10,12,18	4,6,9,11,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,10,12,16,17	4,6,9,11,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,10,12	4,6,9,11,15	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,10,12,16,17,18	4,6,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,10,12,14,17	4,6,9,11,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,10,12,14,16,18	4,6,9,11,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,10,12,14,17,18	4,6,9,11,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,10,12,14,16	4,6,9,11,15	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,10,12	4,6,9,11,13	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,10,12,16,17,18	4,6,9,11,13,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,10,12,18	4,6,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,10,12,16,17	4,6,9,11,13,15,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,10,12,14,17,18	4,6,9,11,13,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,10,12,14,16	4,6,9,11,13	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,10,12,14,17	4,6,9,11,13,15,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,10,12,14,16,18	4,6,9,11,13,15,18	$2^{-28.5}$

Table 0.1193 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,17	4,6,8,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,16,18	4,6,8,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,17,18	4,6,8,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,16	4,6,8,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,14,18	4,6,8,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,14,16,17	4,6,8,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,14	4,6,8,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,14,16,17,18	4,6,8,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,17,18	4,6,8,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,16	4,6,8,13	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,17	4,6,8,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,16,18	4,6,8,13,15,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,14	4,6,8,13	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,14,16,17,18	4,6,8,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,14,18	4,6,8,13,15,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,14,16,17	4,6,8,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,12,18	4,6,8,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,12,16,17	4,6,8,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,12	4,6,8,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,12,16,17,18	4,6,8,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,12,14,17	4,6,8,17	2^{-34}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,12,14,16,18	4,6,8,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,12,14,17,18	4,6,8,15,17,18	2^{-34}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,12,14,16	4,6,8,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,12	4,6,8,13	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,12,16,17,18	4,6,8,13,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,12,18	4,6,8,13,15,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,12,16,17	4,6,8,13,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,12,14,17,18	4,6,8,13,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,12,14,16	4,6,8,13	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,12,14,17	4,6,8,13,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,12,14,16,18	4,6,8,13,15,18	2^{-12}

Table 0.1194 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,17,18	4,6,8,11,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,16	4,6,8,11	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,17	4,6,8,11,15,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,16,18	4,6,8,11,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,14	4,6,8,11	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,14,16,17,18	4,6,8,11,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,14,18	4,6,8,11,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,14,16,17	4,6,8,11,15,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,17	4,6,8,11,13,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,16,18	4,6,8,11,13,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,17,18	4,6,8,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,16	4,6,8,11,13,15	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,14,18	4,6,8,11,13,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,14,16,17	4,6,8,11,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,14	4,6,8,11,13,15	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,14,16,17,18	4,6,8,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,12	4,6,8,11	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,12,16,17,18	4,6,8,11,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,12,18	4,6,8,11,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,12,16,17	4,6,8,11,15,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,12,14,17,18	4,6,8,11,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,12,14,16	4,6,8,11	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,12,14,17	4,6,8,11,15,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,12,14,16,18	4,6,8,11,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,12,18	4,6,8,11,13,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,12,16,17	4,6,8,11,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,12	4,6,8,11,13,15	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,12,16,17,18	4,6,8,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,12,14,17	4,6,8,11,13,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,12,14,16,18	4,6,8,11,13,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,12,14,17,18	4,6,8,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,12,14,16	4,6,8,11,13,15	2^{-12}

Table 0.1195 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,10,18	4,6,8,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,10,16,17	4,6,8,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,10	4,6,8,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,10,16,17,18	4,6,8,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,10,14,17	4,6,8,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,10,14,16,18	4,6,8,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,10,14,17,18	4,6,8,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,10,14,16	4,6,8,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,10	4,6,8,13	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,10,16,17,18	4,6,8,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,10,18	4,6,8,13,15,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,10,16,17	4,6,8,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,10,14,17,18	4,6,8,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,10,14,16	4,6,8,13	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,10,14,17	4,6,8,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,10,14,16,18	4,6,8,13,15,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,10,12,17	4,6,8,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,10,12,16,18	4,6,8,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,10,12,17,18	4,6,8,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,10,12,16	4,6,8,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,10,12,14,18	4,6,8,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,10,12,14,16,17	4,6,8,17	2^{-1}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,10,12,14	4,6,8,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,10,12,14,16,17,18	4,6,8,15,17,18	2^{-1}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,10,12,17,18	4,6,8,13,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,10,12,16	4,6,8,13	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,10,12,17	4,6,8,13,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,10,12,16,18	4,6,8,13,15,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,10,12,14	4,6,8,13	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,10,12,14,16,17,18	4,6,8,13,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,10,12,14,18	4,6,8,13,15,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,10,12,14,16,17	4,6,8,13,15,17	$2^{-6.5}$

Table 0.1196 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,10	4,6,8,11	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,10,16,17,18	4,6,8,11,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,10,18	4,6,8,11,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,10,16,17	4,6,8,11,15,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,10,14,17,18	4,6,8,11,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,10,14,16	4,6,8,11	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,10,14,17	4,6,8,11,15,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,10,14,16,18	4,6,8,11,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,10,18	4,6,8,11,13,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,10,16,17	4,6,8,11,13,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,10	4,6,8,11,13,15	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,10,16,17,18	4,6,8,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,10,14,17	4,6,8,11,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,10,14,16,18	4,6,8,11,13,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,10,14,17,18	4,6,8,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,10,14,16	4,6,8,11,13,15	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,10,12,17,18	4,6,8,11,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,10,12,16	4,6,8,11	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,10,12,17	4,6,8,11,15,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,10,12,16,18	4,6,8,11,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,10,12,14	4,6,8,11	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,10,12,14,16,17,18	4,6,8,11,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,10,12,14,18	4,6,8,11,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,10,12,14,16,17	4,6,8,11,15,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,10,12,17	4,6,8,11,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,10,12,16,18	4,6,8,11,13,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,10,12,17,18	4,6,8,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,10,12,16	4,6,8,11,13,15	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,10,12,14,18	4,6,8,11,13,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,10,12,14,16,17	4,6,8,11,13,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,10,12,14	4,6,8,11,13,15	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,10,12,14,16,17,18	4,6,8,11,13,15,17,18	$2^{-6.5}$

Table 0.1197 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,17,18	4,6,8,9,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,16	4,6,8,9	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,17	4,6,8,9,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,16,18	4,6,8,9,15,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,14	4,6,8,9	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,14,16,17,18	4,6,8,9,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,14,18	4,6,8,9,15,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,14,16,17	4,6,8,9,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,17	4,6,8,9,13,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,16,18	4,6,8,9,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,17,18	4,6,8,9,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,16	4,6,8,9,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,14,18	4,6,8,9,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,14,16,17	4,6,8,9,13,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,14	4,6,8,9,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,14,16,17,18	4,6,8,9,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,12	4,6,8,9	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,12,16,17,18	4,6,8,9,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,12,18	4,6,8,9,15,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,12,16,17	4,6,8,9,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,12,14,17,18	4,6,8,9,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,12,14,16	4,6,8,9	2^{-1}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,12,14,17	4,6,8,9,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,12,14,16,18	4,6,8,9,15,18	2^{-1}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,12,18	4,6,8,9,13,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,12,16,17	4,6,8,9,13,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,12	4,6,8,9,13,15	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,12,16,17,18	4,6,8,9,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,12,14,17	4,6,8,9,13,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,12,14,16,18	4,6,8,9,13,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,12,14,17,18	4,6,8,9,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,12,14,16	4,6,8,9,13,15	$2^{-6.5}$

Table 0.1198 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,17	4,6,8,9,11,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,16,18	4,6,8,9,11,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,17,18	4,6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,16	4,6,8,9,11,15	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,14,18	4,6,8,9,11,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,14,16,17	4,6,8,9,11,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,14	4,6,8,9,11,15	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,14,16,17,18	4,6,8,9,11,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,17,18	4,6,8,9,11,13,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,16	4,6,8,9,11,13	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,17	4,6,8,9,11,13,15,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,16,18	4,6,8,9,11,13,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,14	4,6,8,9,11,13	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,14,16,17,18	4,6,8,9,11,13,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,14,18	4,6,8,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,14,16,17	4,6,8,9,11,13,15,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,12,18	4,6,8,9,11,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,12,16,17	4,6,8,9,11,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,12	4,6,8,9,11,15	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,12,16,17,18	4,6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,12,14,17	4,6,8,9,11,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,12,14,16,18	4,6,8,9,11,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,12,14,17,18	4,6,8,9,11,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,12,14,16	4,6,8,9,11,15	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,12	4,6,8,9,11,13	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,12,16,17,18	4,6,8,9,11,13,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,12,18	4,6,8,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,12,16,17	4,6,8,9,11,13,15,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,12,14,17,18	4,6,8,9,11,13,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,12,14,16	4,6,8,9,11,13	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,12,14,17	4,6,8,9,11,13,15,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,12,14,16,18	4,6,8,9,11,13,15,18	$2^{-6.5}$

Table 0.1199 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,10	4,6,8,9	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,10,16,17,18	4,6,8,9,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,10,18	4,6,8,9,15,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,10,16,17	4,6,8,9,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,10,14,17,18	4,6,8,9,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,10,14,16	4,6,8,9	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,10,14,17	4,6,8,9,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,10,14,16,18	4,6,8,9,15,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,10,18	4,6,8,9,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,10,16,17	4,6,8,9,13,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,10	4,6,8,9,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,10,16,17,18	4,6,8,9,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,10,14,17	4,6,8,9,13,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,10,14,16,18	4,6,8,9,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,10,14,17,18	4,6,8,9,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,10,14,16	4,6,8,9,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,10,12,17,18	4,6,8,9,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,10,12,16	4,6,8,9	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,10,12,17	4,6,8,9,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,10,12,16,18	4,6,8,9,15,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,10,12,14	4,6,8,9	2^{-34}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,10,12,14,16,17,18	4,6,8,9,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,10,12,14,18	4,6,8,9,15,18	2^{-34}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,10,12,14,16,17	4,6,8,9,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,10,12,17	4,6,8,9,13,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,10,12,16,18	4,6,8,9,13,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,10,12,17,18	4,6,8,9,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,10,12,16	4,6,8,9,13,15	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,10,12,14,18	4,6,8,9,13,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,10,12,14,16,17	4,6,8,9,13,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,10,12,14	4,6,8,9,13,15	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,10,12,14,16,17,18	4,6,8,9,13,15,17,18	2^{-12}

Table 0.1200 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,10,18	4,6,8,9,11,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,10,16,17	4,6,8,9,11,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,10	4,6,8,9,11,15	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,10,16,17,18	4,6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,10,14,17	4,6,8,9,11,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,10,14,16,18	4,6,8,9,11,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,10,14,17,18	4,6,8,9,11,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,10,14,16	4,6,8,9,11,15	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,10	4,6,8,9,11,13	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,10,16,17,18	4,6,8,9,11,13,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,10,18	4,6,8,9,11,13,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,10,16,17	4,6,8,9,11,13,15,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,10,14,17,18	4,6,8,9,11,13,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,10,14,16	4,6,8,9,11,13	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,10,14,17	4,6,8,9,11,13,15,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,10,14,16,18	4,6,8,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,10,12,17	4,6,8,9,11,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,10,12,16,18	4,6,8,9,11,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,10,12,17,18	4,6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,10,12,16	4,6,8,9,11,15	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,10,12,14,18	4,6,8,9,11,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,10,12,14,16,17	4,6,8,9,11,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,10,12,14	4,6,8,9,11,15	2^{-23}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,10,12,14,16,17,18	4,6,8,9,11,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,10,12,17,18	4,6,8,9,11,13,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,10,12,16	4,6,8,9,11,13	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,10,12,17	4,6,8,9,11,13,15,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,10,12,16,18	4,6,8,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,10,12,14	4,6,8,9,11,13	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,10,12,14,16,17,18	4,6,8,9,11,13,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,10,12,14,18	4,6,8,9,11,13,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,10,12,14,16,17	4,6,8,9,11,13,15,17	2^{-12}

Table 0.1201 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,7	4,6	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,7,16,17,18	4,6,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,7,18	4,6,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,7,16,17	4,6,15,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,7,14,17,18	4,6,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,7,14,16	4,6	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,7,14,17	4,6,15,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,7,14,16,18	4,6,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,7,18	4,6,13,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,7,16,17	4,6,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,7	4,6,13,15	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,7,16,17,18	4,6,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,7,14,17	4,6,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,7,14,16,18	4,6,13,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,7,14,17,18	4,6,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,7,14,16	4,6,13,15	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,7,12,17,18	4,6,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,7,12,16	4,6	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,7,12,17	4,6,15,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,7,12,16,18	4,6,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,7,12,14	4,6	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,7,12,14,16,17,18	4,6,17,18	2^{-34}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,7,12,14,18	4,6,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,7,12,14,16,17	4,6,15,17	2^{-34}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,7,12,17	4,6,13,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,7,12,16,18	4,6,13,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,7,12,17,18	4,6,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,7,12,16	4,6,13,15	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,7,12,14,18	4,6,13,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,7,12,14,16,17	4,6,13,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,7,12,14	4,6,13,15	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,7,12,14,16,17,18	4,6,13,15,17,18	$2^{-28.5}$

Table 0.1202 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,7,18	4,6,11,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,7,16,17	4,6,11,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,7	4,6,11,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,7,16,17,18	4,6,11,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,7,14,17	4,6,11,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,7,14,16,18	4,6,11,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,7,14,17,18	4,6,11,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,7,14,16	4,6,11,15	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,7	4,6,11,13	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,7,16,17,18	4,6,11,13,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,7,18	4,6,11,13,15,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,7,16,17	4,6,11,13,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,7,14,17,18	4,6,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,7,14,16	4,6,11,13	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,7,14,17	4,6,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,7,14,16,18	4,6,11,13,15,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,7,12,17	4,6,11,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,7,12,16,18	4,6,11,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,7,12,17,18	4,6,11,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,7,12,16	4,6,11,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,7,12,14,18	4,6,11,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,7,12,14,16,17	4,6,11,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,7,12,14	4,6,11,15	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,7,12,14,16,17,18	4,6,11,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,7,12,17,18	4,6,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,7,12,16	4,6,11,13	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,7,12,17	4,6,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,7,12,16,18	4,6,11,13,15,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,7,12,14	4,6,11,13	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,7,12,14,16,17,18	4,6,11,13,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,7,12,14,18	4,6,11,13,15,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,7,12,14,16,17	4,6,11,13,15,17	$2^{-28.5}$

Table 0.1203 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,7,10,17,18	4,6,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,7,10,16	4,6	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,7,10,17	4,6,15,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,7,10,16,18	4,6,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,7,10,14	4,6	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,7,10,14,16,17,18	4,6,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,7,10,14,18	4,6,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,7,10,14,16,17	4,6,15,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,7,10,17	4,6,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,7,10,16,18	4,6,13,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,7,10,17,18	4,6,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,7,10,16	4,6,13,15	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,7,10,14,18	4,6,13,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,7,10,14,16,17	4,6,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,7,10,14	4,6,13,15	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,7,10,14,16,17,18	4,6,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,7,10,12	4,6	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,7,10,12,16,17,18	4,6,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,7,10,12,18	4,6,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,7,10,12,16,17	4,6,15,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,7,10,12,14,17,18	4,6,17,18	2^{-1}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,7,10,12,14,16	4,6	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,7,10,12,14,17	4,6,15,17	2^{-1}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,7,10,12,14,16,18	4,6,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,7,10,12,18	4,6,13,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,7,10,12,16,17	4,6,13,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,7,10,12	4,6,13,15	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,7,10,12,16,17,18	4,6,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,7,10,12,14,17	4,6,13,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,7,10,12,14,16,18	4,6,13,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,7,10,12,14,17,18	4,6,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,7,10,12,14,16	4,6,13,15	2^{-23}

Table 0.1204 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,7,10,17	4,6,11,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,7,10,16,18	4,6,11,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,7,10,17,18	4,6,11,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,7,10,16	4,6,11,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,7,10,14,18	4,6,11,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,7,10,14,16,17	4,6,11,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,7,10,14	4,6,11,15	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,7,10,14,16,17,18	4,6,11,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,7,10,17,18	4,6,11,13,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,7,10,16	4,6,11,13	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,7,10,17	4,6,11,13,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,7,10,16,18	4,6,11,13,15,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,7,10,14	4,6,11,13	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,7,10,14,16,17,18	4,6,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,7,10,14,18	4,6,11,13,15,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,7,10,14,16,17	4,6,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,7,10,12,18	4,6,11,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,7,10,12,16,17	4,6,11,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,7,10,12	4,6,11,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,7,10,12,16,17,18	4,6,11,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,7,10,12,14,17	4,6,11,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,7,10,12,14,16,18	4,6,11,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,7,10,12,14,17,18	4,6,11,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,7,10,12,14,16	4,6,11,15	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,7,10,12	4,6,11,13	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,7,10,12,16,17,18	4,6,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,7,10,12,18	4,6,11,13,15,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,7,10,12,16,17	4,6,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,7,10,12,14,17,18	4,6,11,13,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,7,10,12,14,16	4,6,11,13	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,7,10,12,14,17	4,6,11,13,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,7,10,12,14,16,18	4,6,11,13,15,18	2^{-23}

Table 0.1205 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,7,18	4,6,9,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,7,16,17	4,6,9,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,7	4,6,9,15	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,7,16,17,18	4,6,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,7,14,17	4,6,9,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,7,14,16,18	4,6,9,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,7,14,17,18	4,6,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,7,14,16	4,6,9,15	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,7	4,6,9,13	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,7,16,17,18	4,6,9,13,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,7,18	4,6,9,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,7,16,17	4,6,9,13,15,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,7,14,17,18	4,6,9,13,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,7,14,16	4,6,9,13	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,7,14,17	4,6,9,13,15,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,7,14,16,18	4,6,9,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,7,12,17	4,6,9,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,7,12,16,18	4,6,9,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,7,12,17,18	4,6,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,7,12,16	4,6,9,15	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,7,12,14,18	4,6,9,18	2^{-1}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,7,12,14,16,17	4,6,9,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,7,12,14	4,6,9,15	2^{-1}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,7,12,14,16,17,18	4,6,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,7,12,17,18	4,6,9,13,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,7,12,16	4,6,9,13	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,7,12,17	4,6,9,13,15,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,7,12,16,18	4,6,9,13,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,7,12,14	4,6,9,13	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,7,12,14,16,17,18	4,6,9,13,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,7,12,14,18	4,6,9,13,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,7,12,14,16,17	4,6,9,13,15,17	2^{-23}

Table 0.1206 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,7	4,6,9,11	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,7,16,17,18	4,6,9,11,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,7,18	4,6,9,11,15,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,7,16,17	4,6,9,11,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,7,14,17,18	4,6,9,11,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,7,14,16	4,6,9,11	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,7,14,17	4,6,9,11,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,7,14,16,18	4,6,9,11,15,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,7,18	4,6,9,11,13,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,7,16,17	4,6,9,11,13,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,7	4,6,9,11,13,15	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,7,16,17,18	4,6,9,11,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,7,14,17	4,6,9,11,13,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,7,14,16,18	4,6,9,11,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,7,14,17,18	4,6,9,11,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,7,14,16	4,6,9,11,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,7,12,17,18	4,6,9,11,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,7,12,16	4,6,9,11	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,7,12,17	4,6,9,11,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,7,12,16,18	4,6,9,11,15,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,7,12,14	4,6,9,11	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,7,12,14,16,17,18	4,6,9,11,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,7,12,14,18	4,6,9,11,15,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,7,12,14,16,17	4,6,9,11,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,7,12,17	4,6,9,11,13,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,7,12,16,18	4,6,9,11,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,7,12,17,18	4,6,9,11,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,7,12,16	4,6,9,11,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,7,12,14,18	4,6,9,11,13,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,7,12,14,16,17	4,6,9,11,13,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,7,12,14	4,6,9,11,13,15	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,7,12,14,16,17,18	4,6,9,11,13,15,17,18	2^{-23}

Table 0.1207 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,7,10,17	4,6,9,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,7,10,16,18	4,6,9,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,7,10,17,18	4,6,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,7,10,16	4,6,9,15	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,7,10,14,18	4,6,9,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,7,10,14,16,17	4,6,9,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,7,10,14	4,6,9,15	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,7,10,14,16,17,18	4,6,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,7,10,17,18	4,6,9,13,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,7,10,16	4,6,9,13	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,7,10,17	4,6,9,13,15,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,7,10,16,18	4,6,9,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,7,10,14	4,6,9,13	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,7,10,14,16,17,18	4,6,9,13,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,7,10,14,18	4,6,9,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,7,10,14,16,17	4,6,9,13,15,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,7,10,12,18	4,6,9,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,7,10,12,16,17	4,6,9,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,7,10,12	4,6,9,15	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,7,10,12,16,17,18	4,6,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,7,10,12,14,17	4,6,9,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,7,10,12,14,16,18	4,6,9,18	2^{-34}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,7,10,12,14,17,18	4,6,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,7,10,12,14,16	4,6,9,15	2^{-34}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,7,10,12	4,6,9,13	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,7,10,12,16,17,18	4,6,9,13,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,7,10,12,18	4,6,9,13,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,7,10,12,16,17	4,6,9,13,15,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,7,10,12,14,17,18	4,6,9,13,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,7,10,12,14,16	4,6,9,13	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,7,10,12,14,17	4,6,9,13,15,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,7,10,12,14,16,18	4,6,9,13,15,18	$2^{-28.5}$

Table 0.1208 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,7,10,17,18	4,6,9,11,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,7,10,16	4,6,9,11	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,7,10,17	4,6,9,11,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,7,10,16,18	4,6,9,11,15,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,7,10,14	4,6,9,11	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,7,10,14,16,17,18	4,6,9,11,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,7,10,14,18	4,6,9,11,15,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,7,10,14,16,17	4,6,9,11,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,7,10,17	4,6,9,11,13,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,7,10,16,18	4,6,9,11,13,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,7,10,17,18	4,6,9,11,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,7,10,16	4,6,9,11,13,15	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,7,10,14,18	4,6,9,11,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,7,10,14,16,17	4,6,9,11,13,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,7,10,14	4,6,9,11,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,7,10,14,16,17,18	4,6,9,11,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,7,10,12	4,6,9,11	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,7,10,12,16,17,18	4,6,9,11,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,7,10,12,18	4,6,9,11,15,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,7,10,12,16,17	4,6,9,11,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,7,10,12,14,17,18	4,6,9,11,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,7,10,12,14,16	4,6,9,11	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,7,10,12,14,17	4,6,9,11,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,7,10,12,14,16,18	4,6,9,11,15,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,7,10,12,18	4,6,9,11,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,7,10,12,16,17	4,6,9,11,13,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,7,10,12	4,6,9,11,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,7,10,12,16,17,18	4,6,9,11,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,7,10,12,14,17	4,6,9,11,13,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,7,10,12,14,16,18	4,6,9,11,13,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,7,10,12,14,17,18	4,6,9,11,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,7,10,12,14,16	4,6,9,11,13,15	$2^{-28.5}$

Table 0.1209 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,7,17,18	4,6,8,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,7,16	4,6,8	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,7,17	4,6,8,15,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,7,16,18	4,6,8,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,7,14	4,6,8	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,7,14,16,17,18	4,6,8,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,7,14,18	4,6,8,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,7,14,16,17	4,6,8,15,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,7,17	4,6,8,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,7,16,18	4,6,8,13,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,7,17,18	4,6,8,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,7,16	4,6,8,13,15	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,7,14,18	4,6,8,13,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,7,14,16,17	4,6,8,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,7,14	4,6,8,13,15	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,7,14,16,17,18	4,6,8,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,7,12	4,6,8	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,7,12,16,17,18	4,6,8,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,7,12,18	4,6,8,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,7,12,16,17	4,6,8,15,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,7,12,14,17,18	4,6,8,17,18	2^{-34}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,7,12,14,16	4,6,8	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,7,12,14,17	4,6,8,15,17	2^{-34}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,7,12,14,16,18	4,6,8,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,7,12,18	4,6,8,13,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,7,12,16,17	4,6,8,13,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,7,12	4,6,8,13,15	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,7,12,16,17,18	4,6,8,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,7,12,14,17	4,6,8,13,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,7,12,14,16,18	4,6,8,13,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,7,12,14,17,18	4,6,8,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,7,12,14,16	4,6,8,13,15	2^{-12}

Table 0.1210 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,7,17	4,6,8,11,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,7,16,18	4,6,8,11,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,7,17,18	4,6,8,11,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,7,16	4,6,8,11,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,7,14,18	4,6,8,11,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,7,14,16,17	4,6,8,11,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,7,14	4,6,8,11,15	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,7,14,16,17,18	4,6,8,11,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,7,17,18	4,6,8,11,13,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,7,16	4,6,8,11,13	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,7,17	4,6,8,11,13,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,7,16,18	4,6,8,11,13,15,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,7,14	4,6,8,11,13	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,7,14,16,17,18	4,6,8,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,7,14,18	4,6,8,11,13,15,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,7,14,16,17	4,6,8,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,7,12,18	4,6,8,11,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,7,12,16,17	4,6,8,11,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,7,12	4,6,8,11,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,7,12,16,17,18	4,6,8,11,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,7,12,14,17	4,6,8,11,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,7,12,14,16,18	4,6,8,11,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,7,12,14,17,18	4,6,8,11,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,7,12,14,16	4,6,8,11,15	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,7,12	4,6,8,11,13	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,7,12,16,17,18	4,6,8,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,7,12,18	4,6,8,11,13,15,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,7,12,16,17	4,6,8,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,7,12,14,17,18	4,6,8,11,13,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,7,12,14,16	4,6,8,11,13	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,7,12,14,17	4,6,8,11,13,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,7,12,14,16,18	4,6,8,11,13,15,18	2^{-12}

Table 0.1211 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,7,10	4,6,8	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,7,10,16,17,18	4,6,8,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,7,10,18	4,6,8,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,7,10,16,17	4,6,8,15,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,7,10,14,17,18	4,6,8,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,7,10,14,16	4,6,8	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,7,10,14,17	4,6,8,15,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,7,10,14,16,18	4,6,8,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,7,10,18	4,6,8,13,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,7,10,16,17	4,6,8,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,7,10	4,6,8,13,15	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,7,10,16,17,18	4,6,8,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,7,10,14,17	4,6,8,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,7,10,14,16,18	4,6,8,13,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,7,10,14,17,18	4,6,8,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,7,10,14,16	4,6,8,13,15	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,7,10,12,17,18	4,6,8,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,7,10,12,16	4,6,8	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,7,10,12,17	4,6,8,15,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,7,10,12,16,18	4,6,8,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,7,10,12,14	4,6,8	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,7,10,12,14,16,17,18	4,6,8,17,18	2^{-1}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,7,10,12,14,18	4,6,8,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,7,10,12,14,16,17	4,6,8,15,17	2^{-1}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,7,10,12,17	4,6,8,13,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,7,10,12,16,18	4,6,8,13,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,7,10,12,17,18	4,6,8,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,7,10,12,16	4,6,8,13,15	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,7,10,12,14,18	4,6,8,13,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,7,10,12,14,16,17	4,6,8,13,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,7,10,12,14	4,6,8,13,15	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,7,10,12,14,16,17,18	4,6,8,13,15,17,18	$2^{-6.5}$

Table 0.1212 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,7,10,18	4,6,8,11,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,7,10,16,17	4,6,8,11,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,7,10	4,6,8,11,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,7,10,16,17,18	4,6,8,11,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,7,10,14,17	4,6,8,11,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,7,10,14,16,18	4,6,8,11,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,7,10,14,17,18	4,6,8,11,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,7,10,14,16	4,6,8,11,15	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,7,10	4,6,8,11,13	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,7,10,16,17,18	4,6,8,11,13,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,7,10,18	4,6,8,11,13,15,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,7,10,16,17	4,6,8,11,13,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,7,10,14,17,18	4,6,8,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,7,10,14,16	4,6,8,11,13	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,7,10,14,17	4,6,8,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,7,10,14,16,18	4,6,8,11,13,15,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,7,10,12,17	4,6,8,11,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,7,10,12,16,18	4,6,8,11,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,7,10,12,17,18	4,6,8,11,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,7,10,12,16	4,6,8,11,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,7,10,12,14,18	4,6,8,11,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,7,10,12,14,16,17	4,6,8,11,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,7,10,12,14	4,6,8,11,15	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,7,10,12,14,16,17,18	4,6,8,11,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,7,10,12,17,18	4,6,8,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,7,10,12,16	4,6,8,11,13	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,7,10,12,17	4,6,8,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,7,10,12,16,18	4,6,8,11,13,15,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,7,10,12,14	4,6,8,11,13	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,7,10,12,14,16,17,18	4,6,8,11,13,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,7,10,12,14,18	4,6,8,11,13,15,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,7,10,12,14,16,17	4,6,8,11,13,15,17	$2^{-6.5}$

Table 0.1213 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,7,17	4,6,8,9,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,7,16,18	4,6,8,9,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,7,17,18	4,6,8,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,7,16	4,6,8,9,15	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,7,14,18	4,6,8,9,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,7,14,16,17	4,6,8,9,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,7,14	4,6,8,9,15	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,7,14,16,17,18	4,6,8,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,7,17,18	4,6,8,9,13,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,7,16	4,6,8,9,13	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,7,17	4,6,8,9,13,15,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,7,16,18	4,6,8,9,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,7,14	4,6,8,9,13	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,7,14,16,17,18	4,6,8,9,13,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,7,14,18	4,6,8,9,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,7,14,16,17	4,6,8,9,13,15,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,7,12,18	4,6,8,9,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,7,12,16,17	4,6,8,9,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,7,12	4,6,8,9,15	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,7,12,16,17,18	4,6,8,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,7,12,14,17	4,6,8,9,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,7,12,14,16,18	4,6,8,9,18	2^{-1}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,7,12,14,17,18	4,6,8,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,7,12,14,16	4,6,8,9,15	2^{-1}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,7,12	4,6,8,9,13	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,7,12,16,17,18	4,6,8,9,13,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,7,12,18	4,6,8,9,13,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,7,12,16,17	4,6,8,9,13,15,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,7,12,14,17,18	4,6,8,9,13,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,7,12,14,16	4,6,8,9,13	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,7,12,14,17	4,6,8,9,13,15,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,7,12,14,16,18	4,6,8,9,13,15,18	$2^{-6.5}$

Table 0.1214 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,7,17,18	4,6,8,9,11,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,7,16	4,6,8,9,11	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,7,17	4,6,8,9,11,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,7,16,18	4,6,8,9,11,15,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,7,14	4,6,8,9,11	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,7,14,16,17,18	4,6,8,9,11,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,7,14,18	4,6,8,9,11,15,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,7,14,16,17	4,6,8,9,11,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,7,17	4,6,8,9,11,13,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,7,16,18	4,6,8,9,11,13,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,7,17,18	4,6,8,9,11,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,7,16	4,6,8,9,11,13,15	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,7,14,18	4,6,8,9,11,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,7,14,16,17	4,6,8,9,11,13,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,7,14	4,6,8,9,11,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,7,14,16,17,18	4,6,8,9,11,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,7,12	4,6,8,9,11	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,7,12,16,17,18	4,6,8,9,11,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,7,12,18	4,6,8,9,11,15,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,7,12,16,17	4,6,8,9,11,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,7,12,14,17,18	4,6,8,9,11,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,7,12,14,16	4,6,8,9,11	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,7,12,14,17	4,6,8,9,11,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,7,12,14,16,18	4,6,8,9,11,15,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,7,12,18	4,6,8,9,11,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,7,12,16,17	4,6,8,9,11,13,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,7,12	4,6,8,9,11,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,7,12,16,17,18	4,6,8,9,11,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,7,12,14,17	4,6,8,9,11,13,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,7,12,14,16,18	4,6,8,9,11,13,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,7,12,14,17,18	4,6,8,9,11,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,7,12,14,16	4,6,8,9,11,13,15	$2^{-6.5}$

Table 0.1215 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,7,10,18	4,6,8,9,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,7,10,16,17	4,6,8,9,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,7,10	4,6,8,9,15	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,7,10,16,17,18	4,6,8,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,7,10,14,17	4,6,8,9,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,7,10,14,16,18	4,6,8,9,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,7,10,14,17,18	4,6,8,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,7,10,14,16	4,6,8,9,15	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,7,10	4,6,8,9,13	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,7,10,16,17,18	4,6,8,9,13,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,7,10,18	4,6,8,9,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,7,10,16,17	4,6,8,9,13,15,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,7,10,14,17,18	4,6,8,9,13,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,7,10,14,16	4,6,8,9,13	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,7,10,14,17	4,6,8,9,13,15,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,7,10,14,16,18	4,6,8,9,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,7,10,12,17	4,6,8,9,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,7,10,12,16,18	4,6,8,9,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,7,10,12,17,18	4,6,8,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,7,10,12,16	4,6,8,9,15	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,7,10,12,14,18	4,6,8,9,18	2^{-34}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,7,10,12,14,16,17	4,6,8,9,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,7,10,12,14	4,6,8,9,15	2^{-34}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,7,10,12,14,16,17,18	4,6,8,9,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,7,10,12,17,18	4,6,8,9,13,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,7,10,12,16	4,6,8,9,13	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,7,10,12,17	4,6,8,9,13,15,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,7,10,12,16,18	4,6,8,9,13,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,7,10,12,14	4,6,8,9,13	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,7,10,12,14,16,17,18	4,6,8,9,13,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,7,10,12,14,18	4,6,8,9,13,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,7,10,12,14,16,17	4,6,8,9,13,15,17	2^{-12}

Table 0.1216 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,7,10	4,6,8,9,11	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,7,10,16,17,18	4,6,8,9,11,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,7,10,18	4,6,8,9,11,15,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,7,10,16,17	4,6,8,9,11,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,7,10,14,17,18	4,6,8,9,11,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,7,10,14,16	4,6,8,9,11	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,7,10,14,17	4,6,8,9,11,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,7,10,14,16,18	4,6,8,9,11,15,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,7,10,18	4,6,8,9,11,13,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,7,10,16,17	4,6,8,9,11,13,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,7,10	4,6,8,9,11,13,15	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,7,10,16,17,18	4,6,8,9,11,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,7,10,14,17	4,6,8,9,11,13,17	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,7,10,14,16,18	4,6,8,9,11,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,7,10,14,17,18	4,6,8,9,11,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,7,10,14,16	4,6,8,9,11,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,7,10,12,17,18	4,6,8,9,11,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,7,10,12,16	4,6,8,9,11	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,7,10,12,17	4,6,8,9,11,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,7,10,12,16,18	4,6,8,9,11,15,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,7,10,12,14	4,6,8,9,11	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,7,10,12,14,16,17,18	4,6,8,9,11,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,7,10,12,14,18	4,6,8,9,11,15,18	2^{-23}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,7,10,12,14,16,17	4,6,8,9,11,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,7,10,12,17	4,6,8,9,11,13,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,7,10,12,16,18	4,6,8,9,11,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,7,10,12,17,18	4,6,8,9,11,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,7,10,12,16	4,6,8,9,11,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,7,10,12,14,18	4,6,8,9,11,13,18	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,7,10,12,14,16,17	4,6,8,9,11,13,17	2^{-12}
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,7,10,12,14	4,6,8,9,11,13,15	$2^{-28.5}$
$(1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,7,10,12,14,16,17,18	4,6,8,9,11,13,15,17,18	2^{-12}

Table 0.1217 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,5,17,18	4,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,5,16	4	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,5,17	4,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,5,16,18	4,15,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,5,14	4	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,5,14,16,17,18	4,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,5,14,18	4,15,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,5,14,16,17	4,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,5,17	4,13,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,5,16,18	4,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,5,17,18	4,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,5,16	4,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,5,14,18	4,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,5,14,16,17	4,13,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,5,14	4,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,5,14,16,17,18	4,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,5,12	4	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,5,12,16,17,18	4,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,5,12,18	4,15,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,5,12,16,17	4,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,12,14,17,18	4,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,5,12,14,16	4	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,12,14,17	4,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,5,12,14,16,18	4,15,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,5,12,18	4,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,5,12,16,17	4,13,17	2^{-34}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,5,12	4,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,5,12,16,17,18	4,13,15,17,18	2^{-34}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,12,14,17	4,13,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,5,12,14,16,18	4,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,12,14,17,18	4,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,5,12,14,16	4,13,15	$2^{-17.5}$

Table 0.1218 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,5,17	4,11,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,5,16,18	4,11,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,5,17,18	4,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,5,16	4,11,15	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,14,18	4,11,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,5,14,16,17	4,11,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,14	4,11,15	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,5,14,16,17,18	4,11,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,5,17,18	4,11,13,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,5,16	4,11,13	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,5,17	4,11,13,15,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,5,16,18	4,11,13,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,5,14	4,11,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,5,14,16,17,18	4,11,13,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,5,14,18	4,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,5,14,16,17	4,11,13,15,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,5,12,18	4,11,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,5,12,16,17	4,11,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,5,12	4,11,15	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,5,12,16,17,18	4,11,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,5,12,14,17	4,11,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,5,12,14,16,18	4,11,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,5,12,14,17,18	4,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,5,12,14,16	4,11,15	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,5,12	4,11,13	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,5,12,16,17,18	4,11,13,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,5,12,18	4,11,13,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,5,12,16,17	4,11,13,15,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,5,12,14,17,18	4,11,13,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,5,12,14,16	4,11,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,5,12,14,17	4,11,13,15,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,5,12,14,16,18	4,11,13,15,18	$2^{-17.5}$

Table 0.1219 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,5,10	4	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,5,10,16,17,18	4,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,5,10,18	4,15,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,5,10,16,17	4,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,5,10,14,17,18	4,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,5,10,14,16	4	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,5,10,14,17	4,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,5,10,14,16,18	4,15,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,5,10,18	4,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,5,10,16,17	4,13,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,5,10	4,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,5,10,16,17,18	4,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,5,10,14,17	4,13,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,5,10,14,16,18	4,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,5,10,14,17,18	4,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,5,10,14,16	4,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,5,10,12,17,18	4,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,5,10,12,16	4	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,5,10,12,17	4,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,5,10,12,16,18	4,15,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,5,10,12,14	4	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,5,10,12,14,16,17,18	4,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,5,10,12,14,18	4,15,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,5,10,12,14,16,17	4,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,5,10,12,17	4,13,17	2^{-1}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,5,10,12,16,18	4,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,5,10,12,17,18	4,13,15,17,18	2^{-1}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,5,10,12,16	4,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,5,10,12,14,18	4,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,5,10,12,14,16,17	4,13,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,5,10,12,14	4,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,5,10,12,14,16,17,18	4,13,15,17,18	2^{-12}

Table 0.1220 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,5,10,18	4,11,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,5,10,16,17	4,11,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,5,10	4,11,15	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,5,10,16,17,18	4,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,5,10,14,17	4,11,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,5,10,14,16,18	4,11,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,5,10,14,17,18	4,11,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,5,10,14,16	4,11,15	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,5,10	4,11,13	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,5,10,16,17,18	4,11,13,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,5,10,18	4,11,13,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,5,10,16,17	4,11,13,15,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,5,10,14,17,18	4,11,13,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,5,10,14,16	4,11,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,5,10,14,17	4,11,13,15,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,5,10,14,16,18	4,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,5,10,12,17	4,11,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,5,10,12,16,18	4,11,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,5,10,12,17,18	4,11,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,5,10,12,16	4,11,15	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,5,10,12,14,18	4,11,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,5,10,12,14,16,17	4,11,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,5,10,12,14	4,11,15	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,5,10,12,14,16,17,18	4,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,5,10,12,17,18	4,11,13,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,5,10,12,16	4,11,13	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,5,10,12,17	4,11,13,15,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,5,10,12,16,18	4,11,13,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5,10,12,14	4,11,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,5,10,12,14,16,17,18	4,11,13,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5,10,12,14,18	4,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,5,10,12,14,16,17	4,11,13,15,17	2^{-12}

Table 0.1221 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,17	4,9,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,5,16,18	4,9,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,17,18	4,9,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,5,16	4,9,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,14,18	4,9,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,5,14,16,17	4,9,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,14	4,9,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,5,14,16,17,18	4,9,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,17,18	4,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,5,16	4,9,13	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,17	4,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,5,16,18	4,9,13,15,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,5,14	4,9,13	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,5,14,16,17,18	4,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,5,14,18	4,9,13,15,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,5,14,16,17	4,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,5,12,18	4,9,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,5,12,16,17	4,9,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,5,12	4,9,15	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,5,12,16,17,18	4,9,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,5,12,14,17	4,9,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,5,12,14,16,18	4,9,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,5,12,14,17,18	4,9,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,5,12,14,16	4,9,15	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,5,12	4,9,13	2^{-1}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,5,12,16,17,18	4,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,5,12,18	4,9,13,15,18	2^{-1}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,5,12,16,17	4,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,5,12,14,17,18	4,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,5,12,14,16	4,9,13	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,5,12,14,17	4,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,5,12,14,16,18	4,9,13,15,18	2^{-12}

Table 0.1222 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,5,17,18	4,9,11,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,5,16	4,9,11	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,5,17	4,9,11,15,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,5,16,18	4,9,11,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,5,14	4,9,11	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,5,14,16,17,18	4,9,11,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,5,14,18	4,9,11,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,5,14,16,17	4,9,11,15,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,5,17	4,9,11,13,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,5,16,18	4,9,11,13,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,5,17,18	4,9,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,5,16	4,9,11,13,15	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,5,14,18	4,9,11,13,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,5,14,16,17	4,9,11,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,5,14	4,9,11,13,15	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,5,14,16,17,18	4,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,5,12	4,9,11	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,5,12,16,17,18	4,9,11,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,5,12,18	4,9,11,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,5,12,16,17	4,9,11,15,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,5,12,14,17,18	4,9,11,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,5,12,14,16	4,9,11	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,5,12,14,17	4,9,11,15,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,5,12,14,16,18	4,9,11,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,5,12,18	4,9,11,13,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,5,12,16,17	4,9,11,13,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,5,12	4,9,11,13,15	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,5,12,16,17,18	4,9,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,5,12,14,17	4,9,11,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,5,12,14,16,18	4,9,11,13,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,5,12,14,17,18	4,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,5,12,14,16	4,9,11,13,15	2^{-12}

Table 0.1223 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,5,10,18	4,9,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,10,16,17	4,9,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,5,10	4,9,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,10,16,17,18	4,9,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,5,10,14,17	4,9,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,5,10,14,16,18	4,9,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,5,10,14,17,18	4,9,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,5,10,14,16	4,9,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,5,10	4,9,13	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,5,10,16,17,18	4,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,5,10,18	4,9,13,15,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,5,10,16,17	4,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,5,10,14,17,18	4,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,5,10,14,16	4,9,13	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,5,10,14,17	4,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,5,10,14,16,18	4,9,13,15,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,5,10,12,17	4,9,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,5,10,12,16,18	4,9,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,5,10,12,17,18	4,9,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,5,10,12,16	4,9,15	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,5,10,12,14,18	4,9,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,5,10,12,14,16,17	4,9,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,10,12,14	4,9,15	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,5,10,12,14,16,17,18	4,9,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,5,10,12,17,18	4,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,5,10,12,16	4,9,13	2^{-34}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,5,10,12,17	4,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,5,10,12,16,18	4,9,13,15,18	2^{-34}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,10,12,14	4,9,13	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,5,10,12,14,16,17,18	4,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,10,12,14,18	4,9,13,15,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,5,10,12,14,16,17	4,9,13,15,17	$2^{-17.5}$

Table 0.1224 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,5,10	4,9,11	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,5,10,16,17,18	4,9,11,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,5,10,18	4,9,11,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,5,10,16,17	4,9,11,15,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,5,10,14,17,18	4,9,11,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,5,10,14,16	4,9,11	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,5,10,14,17	4,9,11,15,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,5,10,14,16,18	4,9,11,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,5,10,18	4,9,11,13,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,5,10,16,17	4,9,11,13,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,5,10	4,9,11,13,15	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,5,10,16,17,18	4,9,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,5,10,14,17	4,9,11,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,5,10,14,16,18	4,9,11,13,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,5,10,14,17,18	4,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,5,10,14,16	4,9,11,13,15	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,5,10,12,17,18	4,9,11,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,5,10,12,16	4,9,11	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,5,10,12,17	4,9,11,15,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,5,10,12,16,18	4,9,11,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,5,10,12,14	4,9,11	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,5,10,12,14,16,17,18	4,9,11,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,5,10,12,14,18	4,9,11,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,5,10,12,14,16,17	4,9,11,15,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,5,10,12,17	4,9,11,13,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,5,10,12,16,18	4,9,11,13,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,5,10,12,17,18	4,9,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,5,10,12,16	4,9,11,13,15	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,5,10,12,14,18	4,9,11,13,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,5,10,12,14,16,17	4,9,11,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,5,10,12,14	4,9,11,13,15	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,5,10,12,14,16,17,18	4,9,11,13,15,17,18	$2^{-17.5}$

Table 0.1225 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5	4,8	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,5,16,17,18	4,8,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,18	4,8,15,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,5,16,17	4,8,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,5,14,17,18	4,8,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,5,14,16	4,8	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,5,14,17	4,8,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,5,14,16,18	4,8,15,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,5,18	4,8,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,5,16,17	4,8,13,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,5	4,8,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,5,16,17,18	4,8,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,5,14,17	4,8,13,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,5,14,16,18	4,8,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,5,14,17,18	4,8,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,5,14,16	4,8,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,5,12,17,18	4,8,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,5,12,16	4,8	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,5,12,17	4,8,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,5,12,16,18	4,8,15,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,5,12,14	4,8	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,5,12,14,16,17,18	4,8,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,5,12,14,18	4,8,15,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,5,12,14,16,17	4,8,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,5,12,17	4,8,13,17	2^{-34}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,5,12,16,18	4,8,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,5,12,17,18	4,8,13,15,17,18	2^{-34}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,5,12,16	4,8,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,5,12,14,18	4,8,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,12,14,16,17	4,8,13,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,5,12,14	4,8,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,12,14,16,17,18	4,8,13,15,17,18	2^{-23}

Table 0.1226 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,5,18	4,8,11,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,5,16,17	4,8,11,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,5	4,8,11,15	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,5,16,17,18	4,8,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,5,14,17	4,8,11,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,5,14,16,18	4,8,11,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,5,14,17,18	4,8,11,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,5,14,16	4,8,11,15	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,5	4,8,11,13	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,5,16,17,18	4,8,11,13,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,5,18	4,8,11,13,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,5,16,17	4,8,11,13,15,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,5,14,17,18	4,8,11,13,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,5,14,16	4,8,11,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,5,14,17	4,8,11,13,15,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,5,14,16,18	4,8,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,5,12,17	4,8,11,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,5,12,16,18	4,8,11,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,5,12,17,18	4,8,11,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,5,12,16	4,8,11,15	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,5,12,14,18	4,8,11,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,12,14,16,17	4,8,11,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,5,12,14	4,8,11,15	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,5,12,14,16,17,18	4,8,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,5,12,17,18	4,8,11,13,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,5,12,16	4,8,11,13	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,5,12,17	4,8,11,13,15,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,5,12,16,18	4,8,11,13,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,5,12,14	4,8,11,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,5,12,14,16,17,18	4,8,11,13,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,5,12,14,18	4,8,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,5,12,14,16,17	4,8,11,13,15,17	2^{-23}

Table 0.1227 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,5,10,17,18	4,8,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,10,16	4,8	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,5,10,17	4,8,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,10,16,18	4,8,15,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,5,10,14	4,8	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,10,14,16,17,18	4,8,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,5,10,14,18	4,8,15,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,10,14,16,17	4,8,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,5,10,17	4,8,13,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,10,16,18	4,8,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,5,10,17,18	4,8,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,10,16	4,8,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,5,10,14,18	4,8,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,5,10,14,16,17	4,8,13,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,5,10,14	4,8,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,5,10,14,16,17,18	4,8,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,5,10,12	4,8	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,5,10,12,16,17,18	4,8,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,5,10,12,18	4,8,15,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,5,10,12,16,17	4,8,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,5,10,12,14,17,18	4,8,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,5,10,12,14,16	4,8	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,5,10,12,14,17	4,8,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,5,10,12,14,16,18	4,8,15,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,5,10,12,18	4,8,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,5,10,12,16,17	4,8,13,17	2^{-1}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,5,10,12	4,8,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,5,10,12,16,17,18	4,8,13,15,17,18	2^{-1}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,5,10,12,14,17	4,8,13,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,5,10,12,14,16,18	4,8,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,5,10,12,14,17,18	4,8,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,5,10,12,14,16	4,8,13,15	$2^{-17.5}$

Table 0.1228 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,5,10,17	4,8,11,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,5,10,16,18	4,8,11,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,5,10,17,18	4,8,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,5,10,16	4,8,11,15	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,5,10,14,18	4,8,11,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,5,10,14,16,17	4,8,11,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,5,10,14	4,8,11,15	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,5,10,14,16,17,18	4,8,11,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,5,10,17,18	4,8,11,13,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,5,10,16	4,8,11,13	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,5,10,17	4,8,11,13,15,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,5,10,16,18	4,8,11,13,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,5,10,14	4,8,11,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,5,10,14,16,17,18	4,8,11,13,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,5,10,14,18	4,8,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,5,10,14,16,17	4,8,11,13,15,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,5,10,12,18	4,8,11,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,5,10,12,16,17	4,8,11,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,5,10,12	4,8,11,15	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,5,10,12,16,17,18	4,8,11,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,5,10,12,14,17	4,8,11,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,5,10,12,14,16,18	4,8,11,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,5,10,12,14,17,18	4,8,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,5,10,12,14,16	4,8,11,15	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,5,10,12	4,8,11,13	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,5,10,12,16,17,18	4,8,11,13,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,5,10,12,18	4,8,11,13,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,5,10,12,16,17	4,8,11,13,15,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,5,10,12,14,17,18	4,8,11,13,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,5,10,12,14,16	4,8,11,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,5,10,12,14,17	4,8,11,13,15,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,5,10,12,14,16,18	4,8,11,13,15,18	$2^{-17.5}$

Table 0.1229 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,5,18	4,8,9,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,5,16,17	4,8,9,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,5	4,8,9,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,5,16,17,18	4,8,9,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,5,14,17	4,8,9,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,5,14,16,18	4,8,9,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,5,14,17,18	4,8,9,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,5,14,16	4,8,9,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,5	4,8,9,13	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,5,16,17,18	4,8,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,5,18	4,8,9,13,15,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,5,16,17	4,8,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,5,14,17,18	4,8,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,5,14,16	4,8,9,13	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,5,14,17	4,8,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,5,14,16,18	4,8,9,13,15,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,5,12,17	4,8,9,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,5,12,16,18	4,8,9,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,5,12,17,18	4,8,9,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,5,12,16	4,8,9,15	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,5,12,14,18	4,8,9,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,5,12,14,16,17	4,8,9,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,5,12,14	4,8,9,15	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,5,12,14,16,17,18	4,8,9,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,5,12,17,18	4,8,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,5,12,16	4,8,9,13	2^{-1}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,5,12,17	4,8,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,5,12,16,18	4,8,9,13,15,18	2^{-1}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,5,12,14	4,8,9,13	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,5,12,14,16,17,18	4,8,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,5,12,14,18	4,8,9,13,15,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,5,12,14,16,17	4,8,9,13,15,17	$2^{-17.5}$

Table 0.1230 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,5	4,8,9,11	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,5,16,17,18	4,8,9,11,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,5,18	4,8,9,11,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,5,16,17	4,8,9,11,15,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,5,14,17,18	4,8,9,11,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,5,14,16	4,8,9,11	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,5,14,17	4,8,9,11,15,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,5,14,16,18	4,8,9,11,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,5,18	4,8,9,11,13,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,5,16,17	4,8,9,11,13,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,5	4,8,9,11,13,15	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,5,16,17,18	4,8,9,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,5,14,17	4,8,9,11,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,5,14,16,18	4,8,9,11,13,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,5,14,17,18	4,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,5,14,16	4,8,9,11,13,15	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,5,12,17,18	4,8,9,11,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,5,12,16	4,8,9,11	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,5,12,17	4,8,9,11,15,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,5,12,16,18	4,8,9,11,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,5,12,14	4,8,9,11	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,5,12,14,16,17,18	4,8,9,11,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,5,12,14,18	4,8,9,11,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,5,12,14,16,17	4,8,9,11,15,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,5,12,17	4,8,9,11,13,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,5,12,16,18	4,8,9,11,13,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,5,12,17,18	4,8,9,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,5,12,16	4,8,9,11,13,15	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,5,12,14,18	4,8,9,11,13,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5,12,14,16,17	4,8,9,11,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,5,12,14	4,8,9,11,13,15	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5,12,14,16,17,18	4,8,9,11,13,15,17,18	$2^{-17.5}$

Table 0.1231 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,5,10,17	4,8,9,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,5,10,16,18	4,8,9,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,5,10,17,18	4,8,9,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,5,10,16	4,8,9,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,5,10,14,18	4,8,9,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,5,10,14,16,17	4,8,9,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,5,10,14	4,8,9,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,5,10,14,16,17,18	4,8,9,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,5,10,17,18	4,8,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,5,10,16	4,8,9,13	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,5,10,17	4,8,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,5,10,16,18	4,8,9,13,15,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,5,10,14	4,8,9,13	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,5,10,14,16,17,18	4,8,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,5,10,14,18	4,8,9,13,15,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,5,10,14,16,17	4,8,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,5,10,12,18	4,8,9,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,5,10,12,16,17	4,8,9,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,5,10,12	4,8,9,15	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,5,10,12,16,17,18	4,8,9,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,5,10,12,14,17	4,8,9,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,10,12,14,16,18	4,8,9,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,5,10,12,14,17,18	4,8,9,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,10,12,14,16	4,8,9,15	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,5,10,12	4,8,9,13	2^{-34}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,5,10,12,16,17,18	4,8,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,5,10,12,18	4,8,9,13,15,18	2^{-34}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,5,10,12,16,17	4,8,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,5,10,12,14,17,18	4,8,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,10,12,14,16	4,8,9,13	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,5,10,12,14,17	4,8,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,10,12,14,16,18	4,8,9,13,15,18	2^{-23}

Table 0.1232 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,5,10,17,18	4,8,9,11,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,5,10,16	4,8,9,11	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,5,10,17	4,8,9,11,15,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,5,10,16,18	4,8,9,11,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,5,10,14	4,8,9,11	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,10,14,16,17,18	4,8,9,11,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,5,10,14,18	4,8,9,11,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,10,14,16,17	4,8,9,11,15,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,5,10,17	4,8,9,11,13,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,5,10,16,18	4,8,9,11,13,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,5,10,17,18	4,8,9,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,5,10,16	4,8,9,11,13,15	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,5,10,14,18	4,8,9,11,13,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,5,10,14,16,17	4,8,9,11,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,5,10,14	4,8,9,11,13,15	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,5,10,14,16,17,18	4,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,5,10,12	4,8,9,11	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,5,10,12,16,17,18	4,8,9,11,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,5,10,12,18	4,8,9,11,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,5,10,12,16,17	4,8,9,11,15,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,5,10,12,14,17,18	4,8,9,11,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,5,10,12,14,16	4,8,9,11	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,5,10,12,14,17	4,8,9,11,15,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,5,10,12,14,16,18	4,8,9,11,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,5,10,12,18	4,8,9,11,13,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,5,10,12,16,17	4,8,9,11,13,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,5,10,12	4,8,9,11,13,15	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,5,10,12,16,17,18	4,8,9,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,5,10,12,14,17	4,8,9,11,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,5,10,12,14,16,18	4,8,9,11,13,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,5,10,12,14,17,18	4,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,5,10,12,14,16	4,8,9,11,13,15	2^{-23}

Table 0.1233 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,5,7,17	4,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,5,7,16,18	4,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,5,7,17,18	4,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,5,7,16	4,15	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,5,7,14,18	4,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,5,7,14,16,17	4,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,5,7,14	4,15	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,5,7,14,16,17,18	4,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,5,7,17,18	4,13,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,5,7,16	4,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,5,7,17	4,13,15,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,5,7,16,18	4,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,5,7,14	4,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,5,7,14,16,17,18	4,13,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,5,7,14,18	4,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,5,7,14,16,17	4,13,15,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,5,7,12,18	4,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,5,7,12,16,17	4,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,5,7,12	4,15	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,5,7,12,16,17,18	4,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,12,14,17	4,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,5,7,12,14,16,18	4,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,5,7,12,14,17,18	4,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,5,7,12,14,16	4,15	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,5,7,12	4,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,5,7,12,16,17,18	4,13,17,18	2^{-34}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,5,7,12,18	4,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,5,7,12,16,17	4,13,15,17	2^{-34}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,5,7,12,14,17,18	4,13,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,5,7,12,14,16	4,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,5,7,12,14,17	4,13,15,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,5,7,12,14,16,18	4,13,15,18	$2^{-17.5}$

Table 0.1234 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,17,18	4,11,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,16	4,11	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,17	4,11,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,16,18	4,11,15,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,14	4,11	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,5,7,14,16,17,18	4,11,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,14,18	4,11,15,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,5,7,14,16,17	4,11,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,17	4,11,13,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,5,7,16,18	4,11,13,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,17,18	4,11,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,5,7,16	4,11,13,15	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,5,7,14,18	4,11,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,5,7,14,16,17	4,11,13,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,5,7,14	4,11,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,5,7,14,16,17,18	4,11,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,5,7,12	4,11	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,5,7,12,16,17,18	4,11,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,5,7,12,18	4,11,15,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,5,7,12,16,17	4,11,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,5,7,12,14,17,18	4,11,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,5,7,12,14,16	4,11	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,5,7,12,14,17	4,11,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,5,7,12,14,16,18	4,11,15,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,5,7,12,18	4,11,13,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,5,7,12,16,17	4,11,13,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,5,7,12	4,11,13,15	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,5,7,12,16,17,18	4,11,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,12,14,17	4,11,13,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,5,7,12,14,16,18	4,11,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,5,7,12,14,17,18	4,11,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,5,7,12,14,16	4,11,13,15	$2^{-17.5}$

Table 0.1235 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,5,7,10,18	4,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,5,7,10,16,17	4,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,5,7,10	4,15	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,5,7,10,16,17,18	4,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,5,7,10,14,17	4,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,5,7,10,14,16,18	4,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,5,7,10,14,17,18	4,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,5,7,10,14,16	4,15	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,5,7,10	4,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,5,7,10,16,17,18	4,13,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,5,7,10,18	4,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,5,7,10,16,17	4,13,15,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,5,7,10,14,17,18	4,13,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,5,7,10,14,16	4,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,5,7,10,14,17	4,13,15,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,5,7,10,14,16,18	4,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,5,7,10,12,17	4,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,5,7,10,12,16,18	4,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,5,7,10,12,17,18	4,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,5,7,10,12,16	4,15	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,5,7,10,12,14,18	4,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,5,7,10,12,14,16,17	4,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,5,7,10,12,14	4,15	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,5,7,10,12,14,16,17,18	4,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,5,7,10,12,17,18	4,13,17,18	2^{-1}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,5,7,10,12,16	4,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,5,7,10,12,17	4,13,15,17	2^{-1}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,5,7,10,12,16,18	4,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,5,7,10,12,14	4,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,5,7,10,12,14,16,17,18	4,13,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,5,7,10,12,14,18	4,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,5,7,10,12,14,16,17	4,13,15,17	2^{-12}

Table 0.1236 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,5,7,10	4,11	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,7,10,16,17,18	4,11,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,5,7,10,18	4,11,15,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,7,10,16,17	4,11,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,10,14,17,18	4,11,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,5,7,10,14,16	4,11	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,10,14,17	4,11,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,5,7,10,14,16,18	4,11,15,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,5,7,10,18	4,11,13,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,5,7,10,16,17	4,11,13,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,5,7,10	4,11,13,15	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,5,7,10,16,17,18	4,11,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,5,7,10,14,17	4,11,13,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,5,7,10,14,16,18	4,11,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,5,7,10,14,17,18	4,11,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,5,7,10,14,16	4,11,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,10,12,17,18	4,11,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,5,7,10,12,16	4,11	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,10,12,17	4,11,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,10,12,16,18	4,11,15,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,7,10,12,14	4,11	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,5,7,10,12,14,16,17,18	4,11,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,5,7,10,12,14,18	4,11,15,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,5,7,10,12,14,16,17	4,11,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,5,7,10,12,17	4,11,13,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,5,7,10,12,16,18	4,11,13,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,5,7,10,12,17,18	4,11,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,5,7,10,12,16	4,11,13,15	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,7,10,12,14,18	4,11,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,5,7,10,12,14,16,17	4,11,13,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,7,10,12,14	4,11,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,5,7,10,12,14,16,17,18	4,11,13,15,17,18	2^{-12}

Table 0.1237 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,5,7,17,18	4,9,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,5,7,16	4,9	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,5,7,17	4,9,15,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,5,7,16,18	4,9,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,7,14	4,9	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,5,7,14,16,17,18	4,9,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,7,14,18	4,9,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,5,7,14,16,17	4,9,15,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,5,7,17	4,9,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,5,7,16,18	4,9,13,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,5,7,17,18	4,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,5,7,16	4,9,13,15	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,5,7,14,18	4,9,13,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,5,7,14,16,17	4,9,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,5,7,14	4,9,13,15	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,5,7,14,16,17,18	4,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,5,7,12	4,9	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,5,7,12,16,17,18	4,9,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,5,7,12,18	4,9,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,5,7,12,16,17	4,9,15,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,5,7,12,14,17,18	4,9,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,5,7,12,14,16	4,9	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,5,7,12,14,17	4,9,15,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,5,7,12,14,16,18	4,9,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,5,7,12,18	4,9,13,18	2^{-1}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,5,7,12,16,17	4,9,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,5,7,12	4,9,13,15	2^{-1}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,5,7,12,16,17,18	4,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,5,7,12,14,17	4,9,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,5,7,12,14,16,18	4,9,13,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,5,7,12,14,17,18	4,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,5,7,12,14,16	4,9,13,15	2^{-12}

Table 0.1238 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,5,7,17	4,9,11,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,5,7,16,18	4,9,11,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,5,7,17,18	4,9,11,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,5,7,16	4,9,11,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,5,7,14,18	4,9,11,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,5,7,14,16,17	4,9,11,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,5,7,14	4,9,11,15	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,5,7,14,16,17,18	4,9,11,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,5,7,17,18	4,9,11,13,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,5,7,16	4,9,11,13	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,5,7,17	4,9,11,13,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,5,7,16,18	4,9,11,13,15,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,5,7,14	4,9,11,13	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,5,7,14,16,17,18	4,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,5,7,14,18	4,9,11,13,15,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,5,7,14,16,17	4,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,5,7,12,18	4,9,11,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,5,7,12,16,17	4,9,11,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,5,7,12	4,9,11,15	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,5,7,12,16,17,18	4,9,11,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,12,14,17	4,9,11,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,5,7,12,14,16,18	4,9,11,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,12,14,17,18	4,9,11,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,5,7,12,14,16	4,9,11,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,5,7,12	4,9,11,13	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,5,7,12,16,17,18	4,9,11,13,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,5,7,12,18	4,9,11,13,15,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,5,7,12,16,17	4,9,11,13,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,7,12,14,17,18	4,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,5,7,12,14,16	4,9,11,13	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,7,12,14,17	4,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,5,7,12,14,16,18	4,9,11,13,15,18	2^{-12}

Table 0.1239 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,5,7,10	4,9	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,5,7,10,16,17,18	4,9,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,5,7,10,18	4,9,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,5,7,10,16,17	4,9,15,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,5,7,10,14,17,18	4,9,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,5,7,10,14,16	4,9	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,5,7,10,14,17	4,9,15,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,5,7,10,14,16,18	4,9,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,5,7,10,18	4,9,13,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,5,7,10,16,17	4,9,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,5,7,10	4,9,13,15	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,5,7,10,16,17,18	4,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,10,14,17	4,9,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,5,7,10,14,16,18	4,9,13,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,10,14,17,18	4,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,5,7,10,14,16	4,9,13,15	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,5,7,10,12,17,18	4,9,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,5,7,10,12,16	4,9	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,5,7,10,12,17	4,9,15,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,5,7,10,12,16,18	4,9,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,5,7,10,12,14	4,9	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,5,7,10,12,14,16,17,18	4,9,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,5,7,10,12,14,18	4,9,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,5,7,10,12,14,16,17	4,9,15,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,5,7,10,12,17	4,9,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,5,7,10,12,16,18	4,9,13,18	2^{-34}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,5,7,10,12,17,18	4,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,5,7,10,12,16	4,9,13,15	2^{-34}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5,7,10,12,14,18	4,9,13,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,5,7,10,12,14,16,17	4,9,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5,7,10,12,14	4,9,13,15	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,5,7,10,12,14,16,17,18	4,9,13,15,17,18	$2^{-17.5}$

Table 0.1240 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,5,7,10,18	4,9,11,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,5,7,10,16,17	4,9,11,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,5,7,10	4,9,11,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,5,7,10,16,17,18	4,9,11,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,5,7,10,14,17	4,9,11,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,5,7,10,14,16,18	4,9,11,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,5,7,10,14,17,18	4,9,11,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,5,7,10,14,16	4,9,11,15	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,5,7,10	4,9,11,13	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,5,7,10,16,17,18	4,9,11,13,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,5,7,10,18	4,9,11,13,15,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,5,7,10,16,17	4,9,11,13,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,10,14,17,18	4,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,5,7,10,14,16	4,9,11,13	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,5,7,10,14,17	4,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,5,7,10,14,16,18	4,9,11,13,15,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,5,7,10,12,17	4,9,11,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,5,7,10,12,16,18	4,9,11,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,5,7,10,12,17,18	4,9,11,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,5,7,10,12,16	4,9,11,15	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,5,7,10,12,14,18	4,9,11,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,5,7,10,12,14,16,17	4,9,11,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,5,7,10,12,14	4,9,11,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,5,7,10,12,14,16,17,18	4,9,11,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,5,7,10,12,17,18	4,9,11,13,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,5,7,10,12,16	4,9,11,13	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,5,7,10,12,17	4,9,11,13,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,5,7,10,12,16,18	4,9,11,13,15,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,5,7,10,12,14	4,9,11,13	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,5,7,10,12,14,16,17,18	4,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,5,7,10,12,14,18	4,9,11,13,15,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,5,7,10,12,14,16,17	4,9,11,13,15,17	$2^{-17.5}$

Table 0.1241 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,5,7,18	4,8,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,5,7,16,17	4,8,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,5,7	4,8,15	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,5,7,16,17,18	4,8,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,5,7,14,17	4,8,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,5,7,14,16,18	4,8,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,5,7,14,17,18	4,8,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,5,7,14,16	4,8,15	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,5,7	4,8,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,5,7,16,17,18	4,8,13,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,5,7,18	4,8,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,5,7,16,17	4,8,13,15,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,5,7,14,17,18	4,8,13,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,14,16	4,8,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,5,7,14,17	4,8,13,15,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,14,16,18	4,8,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,5,7,12,17	4,8,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,5,7,12,16,18	4,8,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,5,7,12,17,18	4,8,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,5,7,12,16	4,8,15	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,5,7,12,14,18	4,8,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,5,7,12,14,16,17	4,8,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,5,7,12,14	4,8,15	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,5,7,12,14,16,17,18	4,8,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,5,7,12,17,18	4,8,13,17,18	2^{-34}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,5,7,12,16	4,8,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,5,7,12,17	4,8,13,15,17	2^{-34}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,5,7,12,16,18	4,8,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,5,7,12,14	4,8,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5,7,12,14,16,17,18	4,8,13,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,5,7,12,14,18	4,8,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5,7,12,14,16,17	4,8,13,15,17	2^{-23}

Table 0.1242 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,5,7	4,8,11	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,5,7,16,17,18	4,8,11,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,5,7,18	4,8,11,15,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,5,7,16,17	4,8,11,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,5,7,14,17,18	4,8,11,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,5,7,14,16	4,8,11	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,5,7,14,17	4,8,11,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,5,7,14,16,18	4,8,11,15,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,5,7,18	4,8,11,13,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,5,7,16,17	4,8,11,13,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,5,7	4,8,11,13,15	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,5,7,16,17,18	4,8,11,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,5,7,14,17	4,8,11,13,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,5,7,14,16,18	4,8,11,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,5,7,14,17,18	4,8,11,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,5,7,14,16	4,8,11,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,5,7,12,17,18	4,8,11,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,5,7,12,16	4,8,11	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,5,7,12,17	4,8,11,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,5,7,12,16,18	4,8,11,15,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,5,7,12,14	4,8,11	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,7,12,14,16,17,18	4,8,11,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,5,7,12,14,18	4,8,11,15,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,5,7,12,14,16,17	4,8,11,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,5,7,12,17	4,8,11,13,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,5,7,12,16,18	4,8,11,13,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,5,7,12,17,18	4,8,11,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,5,7,12,16	4,8,11,13,15	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,5,7,12,14,18	4,8,11,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,5,7,12,14,16,17	4,8,11,13,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,5,7,12,14	4,8,11,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,5,7,12,14,16,17,18	4,8,11,13,15,17,18	2^{-23}

Table 0.1243 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,5,7,10,17	4,8,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,5,7,10,16,18	4,8,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,5,7,10,17,18	4,8,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,5,7,10,16	4,8,15	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,5,7,10,14,18	4,8,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,7,10,14,16,17	4,8,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,5,7,10,14	4,8,15	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,7,10,14,16,17,18	4,8,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,5,7,10,17,18	4,8,13,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,5,7,10,16	4,8,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,5,7,10,17	4,8,13,15,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,5,7,10,16,18	4,8,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,5,7,10,14	4,8,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,5,7,10,14,16,17,18	4,8,13,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,5,7,10,14,18	4,8,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,5,7,10,14,16,17	4,8,13,15,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,5,7,10,12,18	4,8,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,5,7,10,12,16,17	4,8,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,5,7,10,12	4,8,15	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,5,7,10,12,16,17,18	4,8,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,5,7,10,12,14,17	4,8,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,5,7,10,12,14,16,18	4,8,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,5,7,10,12,14,17,18	4,8,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,5,7,10,12,14,16	4,8,15	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,5,7,10,12	4,8,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,5,7,10,12,16,17,18	4,8,13,17,18	2^{-1}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,5,7,10,12,18	4,8,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,5,7,10,12,16,17	4,8,13,15,17	2^{-1}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,5,7,10,12,14,17,18	4,8,13,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,5,7,10,12,14,16	4,8,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,5,7,10,12,14,17	4,8,13,15,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,5,7,10,12,14,16,18	4,8,13,15,18	$2^{-17.5}$

Table 0.1244 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,5,7,10,17,18	4,8,11,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,5,7,10,16	4,8,11	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,5,7,10,17	4,8,11,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,5,7,10,16,18	4,8,11,15,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,5,7,10,14	4,8,11	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,5,7,10,14,16,17,18	4,8,11,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,5,7,10,14,18	4,8,11,15,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,5,7,10,14,16,17	4,8,11,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,5,7,10,17	4,8,11,13,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,5,7,10,16,18	4,8,11,13,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,5,7,10,17,18	4,8,11,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,5,7,10,16	4,8,11,13,15	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,5,7,10,14,18	4,8,11,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,5,7,10,14,16,17	4,8,11,13,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,5,7,10,14	4,8,11,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,5,7,10,14,16,17,18	4,8,11,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,5,7,10,12	4,8,11	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,5,7,10,12,16,17,18	4,8,11,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,5,7,10,12,18	4,8,11,15,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,5,7,10,12,16,17	4,8,11,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,5,7,10,12,14,17,18	4,8,11,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,10,12,14,16	4,8,11	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,5,7,10,12,14,17	4,8,11,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,10,12,14,16,18	4,8,11,15,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,5,7,10,12,18	4,8,11,13,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,5,7,10,12,16,17	4,8,11,13,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,5,7,10,12	4,8,11,13,15	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,5,7,10,12,16,17,18	4,8,11,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,5,7,10,12,14,17	4,8,11,13,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,7,10,12,14,16,18	4,8,11,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,5,7,10,12,14,17,18	4,8,11,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,7,10,12,14,16	4,8,11,13,15	$2^{-17.5}$

Table 0.1245 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,5,7	4,8,9	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,5,7,16,17,18	4,8,9,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,5,7,18	4,8,9,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,5,7,16,17	4,8,9,15,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,5,7,14,17,18	4,8,9,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,5,7,14,16	4,8,9	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,5,7,14,17	4,8,9,15,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,5,7,14,16,18	4,8,9,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,5,7,18	4,8,9,13,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,5,7,16,17	4,8,9,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,5,7	4,8,9,13,15	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,5,7,16,17,18	4,8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,5,7,14,17	4,8,9,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,5,7,14,16,18	4,8,9,13,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,5,7,14,17,18	4,8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,5,7,14,16	4,8,9,13,15	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,5,7,12,17,18	4,8,9,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,5,7,12,16	4,8,9	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,5,7,12,17	4,8,9,15,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,5,7,12,16,18	4,8,9,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,5,7,12,14	4,8,9	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,5,7,12,14,16,17,18	4,8,9,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,5,7,12,14,18	4,8,9,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,5,7,12,14,16,17	4,8,9,15,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,5,7,12,17	4,8,9,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,5,7,12,16,18	4,8,9,13,18	2^{-1}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,5,7,12,17,18	4,8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,5,7,12,16	4,8,9,13,15	2^{-1}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,5,7,12,14,18	4,8,9,13,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,5,7,12,14,16,17	4,8,9,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,5,7,12,14	4,8,9,13,15	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,5,7,12,14,16,17,18	4,8,9,13,15,17,18	$2^{-17.5}$

Table 0.1246 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,7,18	4,8,9,11,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,5,7,16,17	4,8,9,11,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,7	4,8,9,11,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,5,7,16,17,18	4,8,9,11,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,5,7,14,17	4,8,9,11,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,14,16,18	4,8,9,11,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,5,7,14,17,18	4,8,9,11,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,5,7,14,16	4,8,9,11,15	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,5,7	4,8,9,11,13	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,5,7,16,17,18	4,8,9,11,13,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,5,7,18	4,8,9,11,13,15,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,5,7,16,17	4,8,9,11,13,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,5,7,14,17,18	4,8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,14,16	4,8,9,11,13	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,5,7,14,17	4,8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,14,16,18	4,8,9,11,13,15,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,12,17	4,8,9,11,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,12,16,18	4,8,9,11,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,12,17,18	4,8,9,11,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,12,16	4,8,9,11,15	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,5,7,12,14,18	4,8,9,11,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,5,7,12,14,16,17	4,8,9,11,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,5,7,12,14	4,8,9,11,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,5,7,12,14,16,17,18	4,8,9,11,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,5,7,12,17,18	4,8,9,11,13,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,5,7,12,16	4,8,9,11,13	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,5,7,12,17	4,8,9,11,13,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,5,7,12,16,18	4,8,9,11,13,15,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,5,7,12,14	4,8,9,11,13	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,7,12,14,16,17,18	4,8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,5,7,12,14,18	4,8,9,11,13,15,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,7,12,14,16,17	4,8,9,11,13,15,17	$2^{-17.5}$

Table 0.1247 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,5,7,10,17,18	4,8,9,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,5,7,10,16	4,8,9	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,5,7,10,17	4,8,9,15,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,5,7,10,16,18	4,8,9,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,5,7,10,14	4,8,9	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,5,7,10,14,16,17,18	4,8,9,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,5,7,10,14,18	4,8,9,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,5,7,10,14,16,17	4,8,9,15,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,5,7,10,17	4,8,9,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,5,7,10,16,18	4,8,9,13,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,5,7,10,17,18	4,8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,5,7,10,16	4,8,9,13,15	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,5,7,10,14,18	4,8,9,13,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,5,7,10,14,16,17	4,8,9,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,5,7,10,14	4,8,9,13,15	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,5,7,10,14,16,17,18	4,8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,5,7,10,12	4,8,9	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,5,7,10,12,16,17,18	4,8,9,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,5,7,10,12,18	4,8,9,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,5,7,10,12,16,17	4,8,9,15,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,5,7,10,12,14,17,18	4,8,9,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,5,7,10,12,14,16	4,8,9	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,5,7,10,12,14,17	4,8,9,15,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,10,12,14,16,18	4,8,9,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,5,7,10,12,18	4,8,9,13,18	2^{-34}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,5,7,10,12,16,17	4,8,9,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,5,7,10,12	4,8,9,13,15	2^{-34}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,5,7,10,12,16,17,18	4,8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,5,7,10,12,14,17	4,8,9,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,5,7,10,12,14,16,18	4,8,9,13,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,5,7,10,12,14,17,18	4,8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,5,7,10,12,14,16	4,8,9,13,15	2^{-23}

Table 0.1248 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,10,17	4,8,9,11,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,10,16,18	4,8,9,11,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,10,17,18	4,8,9,11,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,10,16	4,8,9,11,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,5,7,10,14,18	4,8,9,11,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,10,14,16,17	4,8,9,11,17	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,5,7,10,14	4,8,9,11,15	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,10,14,16,17,18	4,8,9,11,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,5,7,10,17,18	4,8,9,11,13,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,10,16	4,8,9,11,13	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,5,7,10,17	4,8,9,11,13,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,10,16,18	4,8,9,11,13,15,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,5,7,10,14	4,8,9,11,13	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,5,7,10,14,16,17,18	4,8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,5,7,10,14,18	4,8,9,11,13,15,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,5,7,10,14,16,17	4,8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,5,7,10,12,18	4,8,9,11,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,5,7,10,12,16,17	4,8,9,11,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,5,7,10,12	4,8,9,11,15	$2^{-28.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,5,7,10,12,16,17,18	4,8,9,11,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,5,7,10,12,14,17	4,8,9,11,17	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,5,7,10,12,14,16,18	4,8,9,11,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,5,7,10,12,14,17,18	4,8,9,11,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,5,7,10,12,14,16	4,8,9,11,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,5,7,10,12	4,8,9,11,13	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,5,7,10,12,16,17,18	4,8,9,11,13,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,5,7,10,12,18	4,8,9,11,13,15,18	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,5,7,10,12,16,17	4,8,9,11,13,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,5,7,10,12,14,17,18	4,8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,5,7,10,12,14,16	4,8,9,11,13	2^{-23}
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,5,7,10,12,14,17	4,8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,5,7,10,12,14,16,18	4,8,9,11,13,15,18	2^{-23}

Table 0.1249 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,5	4,6	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,5,16,17,18	4,6,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,5,18	4,6,15,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,5,16,17	4,6,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,5,14,17,18	4,6,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,5,14,16	4,6	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,5,14,17	4,6,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,5,14,16,18	4,6,15,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,5,18	4,6,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,16,17	4,6,13,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,5	4,6,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,5,16,17,18	4,6,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,5,14,17	4,6,13,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,5,14,16,18	4,6,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,5,14,17,18	4,6,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,5,14,16	4,6,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,5,12,17,18	4,6,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,5,12,16	4,6	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,5,12,17	4,6,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,5,12,16,18	4,6,15,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,5,12,14	4,6	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,5,12,14,16,17,18	4,6,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,5,12,14,18	4,6,15,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,5,12,14,16,17	4,6,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,5,12,17	4,6,13,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,5,12,16,18	4,6,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,5,12,17,18	4,6,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,5,12,16	4,6,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,5,12,14,18	4,6,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,5,12,14,16,17	4,6,13,17	2^{-34}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,5,12,14	4,6,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,5,12,14,16,17,18	4,6,13,15,17,18	2^{-34}

Table 0.1250 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,5,18	4,6,11,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,5,16,17	4,6,11,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,5	4,6,11,15	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,5,16,17,18	4,6,11,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,5,14,17	4,6,11,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,5,14,16,18	4,6,11,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,5,14,17,18	4,6,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,5,14,16	4,6,11,15	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5	4,6,11,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,5,16,17,18	4,6,11,13,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5,18	4,6,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,5,16,17	4,6,11,13,15,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,5,14,17,18	4,6,11,13,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,5,14,16	4,6,11,13	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,5,14,17	4,6,11,13,15,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,5,14,16,18	4,6,11,13,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,5,12,17	4,6,11,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,5,12,16,18	4,6,11,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,5,12,17,18	4,6,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,5,12,16	4,6,11,15	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,5,12,14,18	4,6,11,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,5,12,14,16,17	4,6,11,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,5,12,14	4,6,11,15	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,5,12,14,16,17,18	4,6,11,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,5,12,17,18	4,6,11,13,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,5,12,16	4,6,11,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,5,12,17	4,6,11,13,15,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,5,12,16,18	4,6,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,5,12,14	4,6,11,13	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,5,12,14,16,17,18	4,6,11,13,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,5,12,14,18	4,6,11,13,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,5,12,14,16,17	4,6,11,13,15,17	2^{-23}

Table 0.1251 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,10,17,18	4,6,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,5,10,16	4,6	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,10,17	4,6,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,5,10,16,18	4,6,15,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,5,10,14	4,6	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,5,10,14,16,17,18	4,6,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,5,10,14,18	4,6,15,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,5,10,14,16,17	4,6,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,10,17	4,6,13,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,5,10,16,18	4,6,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,10,17,18	4,6,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,5,10,16	4,6,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,5,10,14,18	4,6,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,5,10,14,16,17	4,6,13,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,5,10,14	4,6,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,5,10,14,16,17,18	4,6,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,5,10,12	4,6	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,5,10,12,16,17,18	4,6,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,5,10,12,18	4,6,15,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,5,10,12,16,17	4,6,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,5,10,12,14,17,18	4,6,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,5,10,12,14,16	4,6	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,5,10,12,14,17	4,6,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,5,10,12,14,16,18	4,6,15,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,5,10,12,18	4,6,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,5,10,12,16,17	4,6,13,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,5,10,12	4,6,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,5,10,12,16,17,18	4,6,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,5,10,12,14,17	4,6,13,17	2^{-1}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,5,10,12,14,16,18	4,6,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,5,10,12,14,17,18	4,6,13,15,17,18	2^{-1}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,5,10,12,14,16	4,6,13,15	$2^{-17.5}$

Table 0.1252 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,5,10,17	4,6,11,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,5,10,16,18	4,6,11,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,5,10,17,18	4,6,11,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,5,10,16	4,6,11,15	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,5,10,14,18	4,6,11,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,5,10,14,16,17	4,6,11,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,5,10,14	4,6,11,15	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,5,10,14,16,17,18	4,6,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,5,10,17,18	4,6,11,13,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,5,10,16	4,6,11,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,5,10,17	4,6,11,13,15,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,5,10,16,18	4,6,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,5,10,14	4,6,11,13	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,5,10,14,16,17,18	4,6,11,13,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,5,10,14,18	4,6,11,13,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,5,10,14,16,17	4,6,11,13,15,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,10,12,18	4,6,11,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,5,10,12,16,17	4,6,11,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,10,12	4,6,11,15	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,5,10,12,16,17,18	4,6,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,5,10,12,14,17	4,6,11,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,5,10,12,14,16,18	4,6,11,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,5,10,12,14,17,18	4,6,11,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,5,10,12,14,16	4,6,11,15	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,5,10,12	4,6,11,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,5,10,12,16,17,18	4,6,11,13,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,5,10,12,18	4,6,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,5,10,12,16,17	4,6,11,13,15,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,5,10,12,14,17,18	4,6,11,13,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,5,10,12,14,16	4,6,11,13	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,5,10,12,14,17	4,6,11,13,15,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,5,10,12,14,16,18	4,6,11,13,15,18	$2^{-28.5}$

Table 0.1253 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,5,18	4,6,9,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,5,16,17	4,6,9,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,5	4,6,9,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,5,16,17,18	4,6,9,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,5,14,17	4,6,9,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,5,14,16,18	4,6,9,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,5,14,17,18	4,6,9,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,5,14,16	4,6,9,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5	4,6,9,13	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,5,16,17,18	4,6,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,18	4,6,9,13,15,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,5,16,17	4,6,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,5,14,17,18	4,6,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,5,14,16	4,6,9,13	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,5,14,17	4,6,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,5,14,16,18	4,6,9,13,15,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,5,12,17	4,6,9,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,5,12,16,18	4,6,9,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,5,12,17,18	4,6,9,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,5,12,16	4,6,9,15	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,5,12,14,18	4,6,9,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,12,14,16,17	4,6,9,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,5,12,14	4,6,9,15	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,12,14,16,17,18	4,6,9,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,5,12,17,18	4,6,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,5,12,16	4,6,9,13	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,5,12,17	4,6,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,5,12,16,18	4,6,9,13,15,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,5,12,14	4,6,9,13	2^{-1}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,5,12,14,16,17,18	4,6,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,5,12,14,18	4,6,9,13,15,18	2^{-1}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,5,12,14,16,17	4,6,9,13,15,17	$2^{-17.5}$

Table 0.1254 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,5	4,6,9,11	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,5,16,17,18	4,6,9,11,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,5,18	4,6,9,11,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,5,16,17	4,6,9,11,15,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,5,14,17,18	4,6,9,11,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,5,14,16	4,6,9,11	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,14,17	4,6,9,11,15,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,5,14,16,18	4,6,9,11,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,5,18	4,6,9,11,13,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,5,16,17	4,6,9,11,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,5	4,6,9,11,13,15	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,5,16,17,18	4,6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,5,14,17	4,6,9,11,13,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,5,14,16,18	4,6,9,11,13,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,5,14,17,18	4,6,9,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,5,14,16	4,6,9,11,13,15	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,5,12,17,18	4,6,9,11,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,5,12,16	4,6,9,11	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,5,12,17	4,6,9,11,15,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,5,12,16,18	4,6,9,11,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,5,12,14	4,6,9,11	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,5,12,14,16,17,18	4,6,9,11,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,5,12,14,18	4,6,9,11,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,5,12,14,16,17	4,6,9,11,15,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,5,12,17	4,6,9,11,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,5,12,16,18	4,6,9,11,13,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,5,12,17,18	4,6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,5,12,16	4,6,9,11,13,15	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,5,12,14,18	4,6,9,11,13,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,5,12,14,16,17	4,6,9,11,13,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,5,12,14	4,6,9,11,13,15	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,5,12,14,16,17,18	4,6,9,11,13,15,17,18	$2^{-28.5}$

Table 0.1255 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,5,10,17	4,6,9,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,5,10,16,18	4,6,9,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,5,10,17,18	4,6,9,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,5,10,16	4,6,9,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,5,10,14,18	4,6,9,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,5,10,14,16,17	4,6,9,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,5,10,14	4,6,9,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,5,10,14,16,17,18	4,6,9,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,5,10,17,18	4,6,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,5,10,16	4,6,9,13	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,5,10,17	4,6,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,5,10,16,18	4,6,9,13,15,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,5,10,14	4,6,9,13	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,5,10,14,16,17,18	4,6,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,5,10,14,18	4,6,9,13,15,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,5,10,14,16,17	4,6,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,10,12,18	4,6,9,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,5,10,12,16,17	4,6,9,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,10,12	4,6,9,15	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,5,10,12,16,17,18	4,6,9,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,10,12,14,17	4,6,9,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,5,10,12,14,16,18	4,6,9,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,10,12,14,17,18	4,6,9,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,5,10,12,14,16	4,6,9,15	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,5,10,12	4,6,9,13	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,5,10,12,16,17,18	4,6,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,5,10,12,18	4,6,9,13,15,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,5,10,12,16,17	4,6,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,10,12,14,17,18	4,6,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,5,10,12,14,16	4,6,9,13	2^{-34}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,10,12,14,17	4,6,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,5,10,12,14,16,18	4,6,9,13,15,18	2^{-34}

Table 0.1256 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,5,10,17,18	4,6,9,11,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,5,10,16	4,6,9,11	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,5,10,17	4,6,9,11,15,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,5,10,16,18	4,6,9,11,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,5,10,14	4,6,9,11	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,5,10,14,16,17,18	4,6,9,11,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,5,10,14,18	4,6,9,11,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,5,10,14,16,17	4,6,9,11,15,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,5,10,17	4,6,9,11,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,5,10,16,18	4,6,9,11,13,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,5,10,17,18	4,6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,5,10,16	4,6,9,11,13,15	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,5,10,14,18	4,6,9,11,13,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,5,10,14,16,17	4,6,9,11,13,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,5,10,14	4,6,9,11,13,15	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,5,10,14,16,17,18	4,6,9,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,5,10,12	4,6,9,11	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,5,10,12,16,17,18	4,6,9,11,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,5,10,12,18	4,6,9,11,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,5,10,12,16,17	4,6,9,11,15,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,5,10,12,14,17,18	4,6,9,11,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,5,10,12,14,16	4,6,9,11	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,5,10,12,14,17	4,6,9,11,15,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,5,10,12,14,16,18	4,6,9,11,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,5,10,12,18	4,6,9,11,13,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,5,10,12,16,17	4,6,9,11,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,5,10,12	4,6,9,11,13,15	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,5,10,12,16,17,18	4,6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,5,10,12,14,17	4,6,9,11,13,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,5,10,12,14,16,18	4,6,9,11,13,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,5,10,12,14,17,18	4,6,9,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,5,10,12,14,16	4,6,9,11,13,15	2^{-23}

Table 0.1257 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,5,17,18	4,6,8,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,5,16	4,6,8	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,5,17	4,6,8,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,5,16,18	4,6,8,15,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,5,14	4,6,8	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,5,14,16,17,18	4,6,8,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,5,14,18	4,6,8,15,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,5,14,16,17	4,6,8,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,5,17	4,6,8,13,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,5,16,18	4,6,8,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,5,17,18	4,6,8,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,5,16	4,6,8,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,5,14,18	4,6,8,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,5,14,16,17	4,6,8,13,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,5,14	4,6,8,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,5,14,16,17,18	4,6,8,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,5,12	4,6,8	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,12,16,17,18	4,6,8,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,5,12,18	4,6,8,15,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,12,16,17	4,6,8,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,5,12,14,17,18	4,6,8,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,12,14,16	4,6,8	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,5,12,14,17	4,6,8,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,12,14,16,18	4,6,8,15,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,5,12,18	4,6,8,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,5,12,16,17	4,6,8,13,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,5,12	4,6,8,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,5,12,16,17,18	4,6,8,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,5,12,14,17	4,6,8,13,17	2^{-34}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,12,14,16,18	4,6,8,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,5,12,14,17,18	4,6,8,13,15,17,18	2^{-34}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,12,14,16	4,6,8,13,15	$2^{-17.5}$

Table 0.1258 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,5,17	4,6,8,11,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,5,16,18	4,6,8,11,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,5,17,18	4,6,8,11,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,5,16	4,6,8,11,15	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,5,14,18	4,6,8,11,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,5,14,16,17	4,6,8,11,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,5,14	4,6,8,11,15	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,5,14,16,17,18	4,6,8,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,5,17,18	4,6,8,11,13,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,5,16	4,6,8,11,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,5,17	4,6,8,11,13,15,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,5,16,18	4,6,8,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,5,14	4,6,8,11,13	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,5,14,16,17,18	4,6,8,11,13,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,5,14,18	4,6,8,11,13,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,5,14,16,17	4,6,8,11,13,15,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,5,12,18	4,6,8,11,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,5,12,16,17	4,6,8,11,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,5,12	4,6,8,11,15	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,5,12,16,17,18	4,6,8,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,5,12,14,17	4,6,8,11,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,5,12,14,16,18	4,6,8,11,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,5,12,14,17,18	4,6,8,11,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,5,12,14,16	4,6,8,11,15	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,5,12	4,6,8,11,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,5,12,16,17,18	4,6,8,11,13,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,5,12,18	4,6,8,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,5,12,16,17	4,6,8,11,13,15,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,5,12,14,17,18	4,6,8,11,13,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,5,12,14,16	4,6,8,11,13	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,5,12,14,17	4,6,8,11,13,15,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,5,12,14,16,18	4,6,8,11,13,15,18	$2^{-6.5}$

Table 0.1259 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,5,10	4,6,8	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,5,10,16,17,18	4,6,8,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,5,10,18	4,6,8,15,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,5,10,16,17	4,6,8,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,5,10,14,17,18	4,6,8,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,5,10,14,16	4,6,8	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,5,10,14,17	4,6,8,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,5,10,14,16,18	4,6,8,15,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,5,10,18	4,6,8,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,10,16,17	4,6,8,13,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,5,10	4,6,8,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,10,16,17,18	4,6,8,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,5,10,14,17	4,6,8,13,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,5,10,14,16,18	4,6,8,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,5,10,14,17,18	4,6,8,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,5,10,14,16	4,6,8,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,5,10,12,17,18	4,6,8,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,5,10,12,16	4,6,8	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,5,10,12,17	4,6,8,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,5,10,12,16,18	4,6,8,15,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,5,10,12,14	4,6,8	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,5,10,12,14,16,17,18	4,6,8,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,5,10,12,14,18	4,6,8,15,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,5,10,12,14,16,17	4,6,8,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,5,10,12,17	4,6,8,13,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,10,12,16,18	4,6,8,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,5,10,12,17,18	4,6,8,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,10,12,16	4,6,8,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,10,12,14,18	4,6,8,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,10,12,14,16,17	4,6,8,13,17	2^{-1}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,10,12,14	4,6,8,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,5,10,12,14,16,17,18	4,6,8,13,15,17,18	2^{-1}

Table 0.1260 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,5,10,18	4,6,8,11,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,5,10,16,17	4,6,8,11,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,5,10	4,6,8,11,15	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,5,10,16,17,18	4,6,8,11,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,5,10,14,17	4,6,8,11,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,5,10,14,16,18	4,6,8,11,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,5,10,14,17,18	4,6,8,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,5,10,14,16	4,6,8,11,15	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,5,10	4,6,8,11,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,5,10,16,17,18	4,6,8,11,13,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,5,10,18	4,6,8,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,5,10,16,17	4,6,8,11,13,15,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,5,10,14,17,18	4,6,8,11,13,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,10,14,16	4,6,8,11,13	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,5,10,14,17	4,6,8,11,13,15,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,5,10,14,16,18	4,6,8,11,13,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,5,10,12,17	4,6,8,11,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,5,10,12,16,18	4,6,8,11,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,5,10,12,17,18	4,6,8,11,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,5,10,12,16	4,6,8,11,15	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,5,10,12,14,18	4,6,8,11,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,5,10,12,14,16,17	4,6,8,11,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,5,10,12,14	4,6,8,11,15	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,5,10,12,14,16,17,18	4,6,8,11,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,5,10,12,17,18	4,6,8,11,13,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,5,10,12,16	4,6,8,11,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,5,10,12,17	4,6,8,11,13,15,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,5,10,12,16,18	4,6,8,11,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,5,10,12,14	4,6,8,11,13	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,5,10,12,14,16,17,18	4,6,8,11,13,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,5,10,12,14,18	4,6,8,11,13,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,5,10,12,14,16,17	4,6,8,11,13,15,17	2^{-12}

Table 0.1261 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,5,17	4,6,8,9,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,16,18	4,6,8,9,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,5,17,18	4,6,8,9,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,16	4,6,8,9,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,5,14,18	4,6,8,9,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,5,14,16,17	4,6,8,9,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,5,14	4,6,8,9,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,5,14,16,17,18	4,6,8,9,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,5,17,18	4,6,8,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,16	4,6,8,9,13	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,5,17	4,6,8,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,16,18	4,6,8,9,13,15,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,5,14	4,6,8,9,13	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,5,14,16,17,18	4,6,8,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,5,14,18	4,6,8,9,13,15,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,5,14,16,17	4,6,8,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,5,12,18	4,6,8,9,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,5,12,16,17	4,6,8,9,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,5,12	4,6,8,9,15	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,5,12,16,17,18	4,6,8,9,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,5,12,14,17	4,6,8,9,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,5,12,14,16,18	4,6,8,9,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,5,12,14,17,18	4,6,8,9,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,5,12,14,16	4,6,8,9,15	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,5,12	4,6,8,9,13	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,5,12,16,17,18	4,6,8,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,5,12,18	4,6,8,9,13,15,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,5,12,16,17	4,6,8,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,5,12,14,17,18	4,6,8,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,5,12,14,16	4,6,8,9,13	2^{-1}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,5,12,14,17	4,6,8,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,5,12,14,16,18	4,6,8,9,13,15,18	2^{-1}

Table 0.1262 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,5,17,18	4,6,8,9,11,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,5,16	4,6,8,9,11	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,5,17	4,6,8,9,11,15,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,5,16,18	4,6,8,9,11,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,5,14	4,6,8,9,11	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,5,14,16,17,18	4,6,8,9,11,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,5,14,18	4,6,8,9,11,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,5,14,16,17	4,6,8,9,11,15,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,5,17	4,6,8,9,11,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,5,16,18	4,6,8,9,11,13,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,5,17,18	4,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,5,16	4,6,8,9,11,13,15	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,5,14,18	4,6,8,9,11,13,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,5,14,16,17	4,6,8,9,11,13,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,5,14	4,6,8,9,11,13,15	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,5,14,16,17,18	4,6,8,9,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,5,12	4,6,8,9,11	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,12,16,17,18	4,6,8,9,11,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,5,12,18	4,6,8,9,11,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,12,16,17	4,6,8,9,11,15,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,5,12,14,17,18	4,6,8,9,11,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,5,12,14,16	4,6,8,9,11	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,5,12,14,17	4,6,8,9,11,15,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,5,12,14,16,18	4,6,8,9,11,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,5,12,18	4,6,8,9,11,13,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,5,12,16,17	4,6,8,9,11,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,5,12	4,6,8,9,11,13,15	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,5,12,16,17,18	4,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,5,12,14,17	4,6,8,9,11,13,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,5,12,14,16,18	4,6,8,9,11,13,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,5,12,14,17,18	4,6,8,9,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,5,12,14,16	4,6,8,9,11,13,15	2^{-12}

Table 0.1263 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,5,10,18	4,6,8,9,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,5,10,16,17	4,6,8,9,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,5,10	4,6,8,9,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,5,10,16,17,18	4,6,8,9,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,5,10,14,17	4,6,8,9,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,5,10,14,16,18	4,6,8,9,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,5,10,14,17,18	4,6,8,9,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,5,10,14,16	4,6,8,9,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,10	4,6,8,9,13	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,5,10,16,17,18	4,6,8,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,10,18	4,6,8,9,13,15,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,5,10,16,17	4,6,8,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,5,10,14,17,18	4,6,8,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,5,10,14,16	4,6,8,9,13	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,5,10,14,17	4,6,8,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,5,10,14,16,18	4,6,8,9,13,15,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,5,10,12,17	4,6,8,9,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,5,10,12,16,18	4,6,8,9,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,5,10,12,17,18	4,6,8,9,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,5,10,12,16	4,6,8,9,15	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,5,10,12,14,18	4,6,8,9,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,5,10,12,14,16,17	4,6,8,9,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,5,10,12,14	4,6,8,9,15	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,5,10,12,14,16,17,18	4,6,8,9,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,5,10,12,17,18	4,6,8,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,5,10,12,16	4,6,8,9,13	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,5,10,12,17	4,6,8,9,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,5,10,12,16,18	4,6,8,9,13,15,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,5,10,12,14	4,6,8,9,13	2^{-34}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,5,10,12,14,16,17,18	4,6,8,9,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,5,10,12,14,18	4,6,8,9,13,15,18	2^{-34}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,5,10,12,14,16,17	4,6,8,9,13,15,17	$2^{-17.5}$

Table 0.1264 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,5,10	4,6,8,9,11	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,5,10,16,17,18	4,6,8,9,11,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,5,10,18	4,6,8,9,11,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,5,10,16,17	4,6,8,9,11,15,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,5,10,14,17,18	4,6,8,9,11,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,5,10,14,16	4,6,8,9,11	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,5,10,14,17	4,6,8,9,11,15,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,5,10,14,16,18	4,6,8,9,11,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,5,10,18	4,6,8,9,11,13,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,5,10,16,17	4,6,8,9,11,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,5,10	4,6,8,9,11,13,15	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5,10,16,17,18	4,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,5,10,14,17	4,6,8,9,11,13,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,5,10,14,16,18	4,6,8,9,11,13,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,5,10,14,17,18	4,6,8,9,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,5,10,14,16	4,6,8,9,11,13,15	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,5,10,12,17,18	4,6,8,9,11,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,5,10,12,16	4,6,8,9,11	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,5,10,12,17	4,6,8,9,11,15,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,5,10,12,16,18	4,6,8,9,11,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,5,10,12,14	4,6,8,9,11	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,5,10,12,14,16,17,18	4,6,8,9,11,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,5,10,12,14,18	4,6,8,9,11,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,5,10,12,14,16,17	4,6,8,9,11,15,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,5,10,12,17	4,6,8,9,11,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,5,10,12,16,18	4,6,8,9,11,13,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,5,10,12,17,18	4,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,5,10,12,16	4,6,8,9,11,13,15	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,5,10,12,14,18	4,6,8,9,11,13,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,5,10,12,14,16,17	4,6,8,9,11,13,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,5,10,12,14	4,6,8,9,11,13,15	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,5,10,12,14,16,17,18	4,6,8,9,11,13,15,17,18	$2^{-6.5}$

Table 0.1265 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,5,7,18	4,6,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,5,7,16,17	4,6,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,5,7	4,6,15	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,5,7,16,17,18	4,6,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,5,7,14,17	4,6,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,5,7,14,16,18	4,6,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,5,7,14,17,18	4,6,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,5,7,14,16	4,6,15	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,5,7	4,6,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,5,7,16,17,18	4,6,13,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,5,7,18	4,6,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,5,7,16,17	4,6,13,15,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,5,7,14,17,18	4,6,13,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,5,7,14,16	4,6,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,5,7,14,17	4,6,13,15,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,5,7,14,16,18	4,6,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,5,7,12,17	4,6,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,5,7,12,16,18	4,6,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,5,7,12,17,18	4,6,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,5,7,12,16	4,6,15	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,5,7,12,14,18	4,6,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,5,7,12,14,16,17	4,6,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,5,7,12,14	4,6,15	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,5,7,12,14,16,17,18	4,6,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,5,7,12,17,18	4,6,13,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,5,7,12,16	4,6,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,5,7,12,17	4,6,13,15,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,5,7,12,16,18	4,6,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,5,7,12,14	4,6,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,5,7,12,14,16,17,18	4,6,13,17,18	2^{-34}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,5,7,12,14,18	4,6,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,5,7,12,14,16,17	4,6,13,15,17	2^{-34}

Table 0.1266 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,5,7	4,6,11	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,5,7,16,17,18	4,6,11,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,5,7,18	4,6,11,15,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,5,7,16,17	4,6,11,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,14,17,18	4,6,11,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,14,16	4,6,11	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,14,17	4,6,11,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,14,16,18	4,6,11,15,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,7,18	4,6,11,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,5,7,16,17	4,6,11,13,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,7	4,6,11,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,5,7,16,17,18	4,6,11,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,5,7,14,17	4,6,11,13,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,5,7,14,16,18	4,6,11,13,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,5,7,14,17,18	4,6,11,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,5,7,14,16	4,6,11,13,15	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,12,17,18	4,6,11,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,5,7,12,16	4,6,11	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,12,17	4,6,11,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,5,7,12,16,18	4,6,11,15,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,5,7,12,14	4,6,11	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,7,12,14,16,17,18	4,6,11,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,5,7,12,14,18	4,6,11,15,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,7,12,14,16,17	4,6,11,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,12,17	4,6,11,13,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,5,7,12,16,18	4,6,11,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,12,17,18	4,6,11,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,5,7,12,16	4,6,11,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5,7,12,14,18	4,6,11,13,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,12,14,16,17	4,6,11,13,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5,7,12,14	4,6,11,13,15	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,12,14,16,17,18	4,6,11,13,15,17,18	2^{-23}

Table 0.1267 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,5,7,10,17	4,6,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,5,7,10,16,18	4,6,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,5,7,10,17,18	4,6,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,5,7,10,16	4,6,15	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,5,7,10,14,18	4,6,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,5,7,10,14,16,17	4,6,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,5,7,10,14	4,6,15	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,5,7,10,14,16,17,18	4,6,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,5,7,10,17,18	4,6,13,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,5,7,10,16	4,6,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,5,7,10,17	4,6,13,15,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,5,7,10,16,18	4,6,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,5,7,10,14	4,6,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,5,7,10,14,16,17,18	4,6,13,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,5,7,10,14,18	4,6,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,5,7,10,14,16,17	4,6,13,15,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,5,7,10,12,18	4,6,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,5,7,10,12,16,17	4,6,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,5,7,10,12	4,6,15	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,5,7,10,12,16,17,18	4,6,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,5,7,10,12,14,17	4,6,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,5,7,10,12,14,16,18	4,6,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,5,7,10,12,14,17,18	4,6,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,5,7,10,12,14,16	4,6,15	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,5,7,10,12	4,6,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,5,7,10,12,16,17,18	4,6,13,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,5,7,10,12,18	4,6,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,5,7,10,12,16,17	4,6,13,15,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,5,7,10,12,14,17,18	4,6,13,17,18	2^{-1}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,5,7,10,12,14,16	4,6,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,5,7,10,12,14,17	4,6,13,15,17	2^{-1}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,5,7,10,12,14,16,18	4,6,13,15,18	$2^{-17.5}$

Table 0.1268 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,5,7,10,17,18	4,6,11,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,5,7,10,16	4,6,11	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,5,7,10,17	4,6,11,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,5,7,10,16,18	4,6,11,15,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,5,7,10,14	4,6,11	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,5,7,10,14,16,17,18	4,6,11,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,5,7,10,14,18	4,6,11,15,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,5,7,10,14,16,17	4,6,11,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,5,7,10,17	4,6,11,13,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,5,7,10,16,18	4,6,11,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,5,7,10,17,18	4,6,11,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,5,7,10,16	4,6,11,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,5,7,10,14,18	4,6,11,13,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,5,7,10,14,16,17	4,6,11,13,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,5,7,10,14	4,6,11,13,15	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,5,7,10,14,16,17,18	4,6,11,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,10,12	4,6,11	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,5,7,10,12,16,17,18	4,6,11,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,10,12,18	4,6,11,15,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,5,7,10,12,16,17	4,6,11,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,5,7,10,12,14,17,18	4,6,11,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,10,12,14,16	4,6,11	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,10,12,14,17	4,6,11,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,10,12,14,16,18	4,6,11,15,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,5,7,10,12,18	4,6,11,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,5,7,10,12,16,17	4,6,11,13,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,5,7,10,12	4,6,11,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,5,7,10,12,16,17,18	4,6,11,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,10,12,14,17	4,6,11,13,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,5,7,10,12,14,16,18	4,6,11,13,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,10,12,14,17,18	4,6,11,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,5,7,10,12,14,16	4,6,11,13,15	$2^{-28.5}$

Table 0.1269 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,5,7	4,6,9	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,5,7,16,17,18	4,6,9,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,5,7,18	4,6,9,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,5,7,16,17	4,6,9,15,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,5,7,14,17,18	4,6,9,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,5,7,14,16	4,6,9	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,5,7,14,17	4,6,9,15,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,5,7,14,16,18	4,6,9,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5,7,18	4,6,9,13,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,5,7,16,17	4,6,9,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5,7	4,6,9,13,15	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,5,7,16,17,18	4,6,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,14,17	4,6,9,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,5,7,14,16,18	4,6,9,13,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,14,17,18	4,6,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,5,7,14,16	4,6,9,13,15	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,5,7,12,17,18	4,6,9,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,5,7,12,16	4,6,9	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,5,7,12,17	4,6,9,15,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,5,7,12,16,18	4,6,9,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,5,7,12,14	4,6,9	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,7,12,14,16,17,18	4,6,9,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,5,7,12,14,18	4,6,9,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,7,12,14,16,17	4,6,9,15,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,5,7,12,17	4,6,9,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,5,7,12,16,18	4,6,9,13,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,5,7,12,17,18	4,6,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,5,7,12,16	4,6,9,13,15	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,5,7,12,14,18	4,6,9,13,18	2^{-1}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,5,7,12,14,16,17	4,6,9,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,5,7,12,14	4,6,9,13,15	2^{-1}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,5,7,12,14,16,17,18	4,6,9,13,15,17,18	$2^{-17.5}$

Table 0.1270 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,5,7,18	4,6,9,11,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,5,7,16,17	4,6,9,11,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,5,7	4,6,9,11,15	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,5,7,16,17,18	4,6,9,11,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,5,7,14,17	4,6,9,11,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,5,7,14,16,18	4,6,9,11,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,5,7,14,17,18	4,6,9,11,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,5,7,14,16	4,6,9,11,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,5,7	4,6,9,11,13	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,5,7,16,17,18	4,6,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,5,7,18	4,6,9,11,13,15,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,7,16,17	4,6,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,5,7,14,17,18	4,6,9,11,13,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,5,7,14,16	4,6,9,11,13	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,5,7,14,17	4,6,9,11,13,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,5,7,14,16,18	4,6,9,11,13,15,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,5,7,12,17	4,6,9,11,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,5,7,12,16,18	4,6,9,11,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,5,7,12,17,18	4,6,9,11,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,5,7,12,16	4,6,9,11,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,5,7,12,14,18	4,6,9,11,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,5,7,12,14,16,17	4,6,9,11,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,5,7,12,14	4,6,9,11,15	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,7,12,14,16,17,18	4,6,9,11,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,5,7,12,17,18	4,6,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,5,7,12,16	4,6,9,11,13	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,5,7,12,17	4,6,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,5,7,12,16,18	4,6,9,11,13,15,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,5,7,12,14	4,6,9,11,13	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,5,7,12,14,16,17,18	4,6,9,11,13,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,5,7,12,14,18	4,6,9,11,13,15,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,5,7,12,14,16,17	4,6,9,11,13,15,17	$2^{-28.5}$

Table 0.1271 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,5,7,10,17,18	4,6,9,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,5,7,10,16	4,6,9	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,5,7,10,17	4,6,9,15,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,5,7,10,16,18	4,6,9,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,5,7,10,14	4,6,9	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,5,7,10,14,16,17,18	4,6,9,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,5,7,10,14,18	4,6,9,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,5,7,10,14,16,17	4,6,9,15,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,5,7,10,17	4,6,9,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,5,7,10,16,18	4,6,9,13,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,5,7,10,17,18	4,6,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,5,7,10,16	4,6,9,13,15	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,5,7,10,14,18	4,6,9,13,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,5,7,10,14,16,17	4,6,9,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,5,7,10,14	4,6,9,13,15	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,5,7,10,14,16,17,18	4,6,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,7,10,12	4,6,9	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,5,7,10,12,16,17,18	4,6,9,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,7,10,12,18	4,6,9,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,5,7,10,12,16,17	4,6,9,15,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,5,7,10,12,14,17,18	4,6,9,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,5,7,10,12,14,16	4,6,9	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,5,7,10,12,14,17	4,6,9,15,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,5,7,10,12,14,16,18	4,6,9,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,5,7,10,12,18	4,6,9,13,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,5,7,10,12,16,17	4,6,9,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,5,7,10,12	4,6,9,13,15	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,5,7,10,12,16,17,18	4,6,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,5,7,10,12,14,17	4,6,9,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,5,7,10,12,14,16,18	4,6,9,13,18	2^{-34}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,5,7,10,12,14,17,18	4,6,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,5,7,10,12,14,16	4,6,9,13,15	2^{-34}

Table 0.1272 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,10,17	4,6,9,11,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,5,7,10,16,18	4,6,9,11,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,10,17,18	4,6,9,11,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,5,7,10,16	4,6,9,11,15	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,5,7,10,14,18	4,6,9,11,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,5,7,10,14,16,17	4,6,9,11,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,5,7,10,14	4,6,9,11,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,5,7,10,14,16,17,18	4,6,9,11,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,7,10,17,18	4,6,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,5,7,10,16	4,6,9,11,13	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,7,10,17	4,6,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,5,7,10,16,18	4,6,9,11,13,15,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,5,7,10,14	4,6,9,11,13	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,5,7,10,14,16,17,18	4,6,9,11,13,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,5,7,10,14,18	4,6,9,11,13,15,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,5,7,10,14,16,17	4,6,9,11,13,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,5,7,10,12,18	4,6,9,11,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,5,7,10,12,16,17	4,6,9,11,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,5,7,10,12	4,6,9,11,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,5,7,10,12,16,17,18	4,6,9,11,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,5,7,10,12,14,17	4,6,9,11,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,5,7,10,12,14,16,18	4,6,9,11,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,5,7,10,12,14,17,18	4,6,9,11,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,5,7,10,12,14,16	4,6,9,11,15	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,5,7,10,12	4,6,9,11,13	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,5,7,10,12,16,17,18	4,6,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,5,7,10,12,18	4,6,9,11,13,15,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,5,7,10,12,16,17	4,6,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,5,7,10,12,14,17,18	4,6,9,11,13,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,5,7,10,12,14,16	4,6,9,11,13	2^{-23}
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,5,7,10,12,14,17	4,6,9,11,13,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,5,7,10,12,14,16,18	4,6,9,11,13,15,18	2^{-23}

Table 0.1273 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,5,7,17	4,6,8,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,5,7,16,18	4,6,8,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,5,7,17,18	4,6,8,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,5,7,16	4,6,8,15	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,5,7,14,18	4,6,8,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,5,7,14,16,17	4,6,8,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,5,7,14	4,6,8,15	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,5,7,14,16,17,18	4,6,8,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,5,7,17,18	4,6,8,13,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,5,7,16	4,6,8,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,5,7,17	4,6,8,13,15,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,5,7,16,18	4,6,8,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,5,7,14	4,6,8,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,5,7,14,16,17,18	4,6,8,13,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,5,7,14,18	4,6,8,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,5,7,14,16,17	4,6,8,13,15,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,5,7,12,18	4,6,8,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,7,12,16,17	4,6,8,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,5,7,12	4,6,8,15	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,7,12,16,17,18	4,6,8,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,5,7,12,14,17	4,6,8,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,5,7,12,14,16,18	4,6,8,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,5,7,12,14,17,18	4,6,8,15,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,5,7,12,14,16	4,6,8,15	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,5,7,12	4,6,8,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,5,7,12,16,17,18	4,6,8,13,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,5,7,12,18	4,6,8,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,5,7,12,16,17	4,6,8,13,15,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,5,7,12,14,17,18	4,6,8,13,17,18	2^{-34}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,5,7,12,14,16	4,6,8,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,5,7,12,14,17	4,6,8,13,15,17	2^{-34}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,5,7,12,14,16,18	4,6,8,13,15,18	$2^{-17.5}$

Table 0.1274 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,5,7,17,18	4,6,8,11,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,16	4,6,8,11	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,5,7,17	4,6,8,11,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,16,18	4,6,8,11,15,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,5,7,14	4,6,8,11	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,5,7,14,16,17,18	4,6,8,11,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,5,7,14,18	4,6,8,11,15,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,5,7,14,16,17	4,6,8,11,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,5,7,17	4,6,8,11,13,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,7,16,18	4,6,8,11,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,5,7,17,18	4,6,8,11,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,7,16	4,6,8,11,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,5,7,14,18	4,6,8,11,13,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,5,7,14,16,17	4,6,8,11,13,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,5,7,14	4,6,8,11,13,15	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,5,7,14,16,17,18	4,6,8,11,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,5,7,12	4,6,8,11	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,5,7,12,16,17,18	4,6,8,11,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,5,7,12,18	4,6,8,11,15,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,5,7,12,16,17	4,6,8,11,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,5,7,12,14,17,18	4,6,8,11,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,5,7,12,14,16	4,6,8,11	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,5,7,12,14,17	4,6,8,11,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,5,7,12,14,16,18	4,6,8,11,15,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,5,7,12,18	4,6,8,11,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,5,7,12,16,17	4,6,8,11,13,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,5,7,12	4,6,8,11,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,5,7,12,16,17,18	4,6,8,11,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,5,7,12,14,17	4,6,8,11,13,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,5,7,12,14,16,18	4,6,8,11,13,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,5,7,12,14,17,18	4,6,8,11,13,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,5,7,12,14,16	4,6,8,11,13,15	$2^{-6.5}$

Table 0.1275 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,5,7,10,18	4,6,8,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,5,7,10,16,17	4,6,8,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,5,7,10	4,6,8,15	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,5,7,10,16,17,18	4,6,8,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,5,7,10,14,17	4,6,8,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,5,7,10,14,16,18	4,6,8,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,5,7,10,14,17,18	4,6,8,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,5,7,10,14,16	4,6,8,15	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,5,7,10	4,6,8,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5,7,10,16,17,18	4,6,8,13,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,5,7,10,18	4,6,8,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5,7,10,16,17	4,6,8,13,15,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,5,7,10,14,17,18	4,6,8,13,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,5,7,10,14,16	4,6,8,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,5,7,10,14,17	4,6,8,13,15,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,5,7,10,14,16,18	4,6,8,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,5,7,10,12,17	4,6,8,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,5,7,10,12,16,18	4,6,8,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,5,7,10,12,17,18	4,6,8,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,5,7,10,12,16	4,6,8,15	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,5,7,10,12,14,18	4,6,8,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,5,7,10,12,14,16,17	4,6,8,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,5,7,10,12,14	4,6,8,15	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,5,7,10,12,14,16,17,18	4,6,8,15,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,5,7,10,12,17,18	4,6,8,13,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,5,7,10,12,16	4,6,8,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,5,7,10,12,17	4,6,8,13,15,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,10,12,16,18	4,6,8,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,5,7,10,12,14	4,6,8,13	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,5,7,10,12,14,16,17,18	4,6,8,13,17,18	2^{-1}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,5,7,10,12,14,18	4,6,8,13,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,5,7,10,12,14,16,17	4,6,8,13,15,17	2^{-1}

Table 0.1276 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,5,7,10	4,6,8,11	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,5,7,10,16,17,18	4,6,8,11,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,5,7,10,18	4,6,8,11,15,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,5,7,10,16,17	4,6,8,11,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,5,7,10,14,17,18	4,6,8,11,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,5,7,10,14,16	4,6,8,11	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,5,7,10,14,17	4,6,8,11,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,5,7,10,14,16,18	4,6,8,11,15,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,7,10,18	4,6,8,11,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,5,7,10,16,17	4,6,8,11,13,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,5,7,10	4,6,8,11,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,5,7,10,16,17,18	4,6,8,11,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,5,7,10,14,17	4,6,8,11,13,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,5,7,10,14,16,18	4,6,8,11,13,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,5,7,10,14,17,18	4,6,8,11,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,5,7,10,14,16	4,6,8,11,13,15	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,5,7,10,12,17,18	4,6,8,11,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,5,7,10,12,16	4,6,8,11	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,5,7,10,12,17	4,6,8,11,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,5,7,10,12,16,18	4,6,8,11,15,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,5,7,10,12,14	4,6,8,11	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,5,7,10,12,14,16,17,18	4,6,8,11,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,5,7,10,12,14,18	4,6,8,11,15,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,5,7,10,12,14,16,17	4,6,8,11,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,5,7,10,12,17	4,6,8,11,13,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,5,7,10,12,16,18	4,6,8,11,13,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,5,7,10,12,17,18	4,6,8,11,13,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,5,7,10,12,16	4,6,8,11,13,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,5,7,10,12,14,18	4,6,8,11,13,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,5,7,10,12,14,16,17	4,6,8,11,13,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,5,7,10,12,14	4,6,8,11,13,15	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,5,7,10,12,14,16,17,18	4,6,8,11,13,15,17,18	2^{-12}

Table 0.1277 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,5,7,17,18	4,6,8,9,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,16	4,6,8,9	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,17	4,6,8,9,15,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,16,18	4,6,8,9,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,5,7,14	4,6,8,9	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,5,7,14,16,17,18	4,6,8,9,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,5,7,14,18	4,6,8,9,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,5,7,14,16,17	4,6,8,9,15,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,5,7,17	4,6,8,9,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,5,7,16,18	4,6,8,9,13,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,5,7,17,18	4,6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,5,7,16	4,6,8,9,13,15	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,5,7,14,18	4,6,8,9,13,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,5,7,14,16,17	4,6,8,9,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,5,7,14	4,6,8,9,13,15	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,5,7,14,16,17,18	4,6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,5,7,12	4,6,8,9	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,5,7,12,16,17,18	4,6,8,9,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,5,7,12,18	4,6,8,9,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,5,7,12,16,17	4,6,8,9,15,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,5,7,12,14,17,18	4,6,8,9,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,5,7,12,14,16	4,6,8,9	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,5,7,12,14,17	4,6,8,9,15,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,5,7,12,14,16,18	4,6,8,9,15,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,5,7,12,18	4,6,8,9,13,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,5,7,12,16,17	4,6,8,9,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,5,7,12	4,6,8,9,13,15	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,5,7,12,16,17,18	4,6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,5,7,12,14,17	4,6,8,9,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,5,7,12,14,16,18	4,6,8,9,13,18	2^{-1}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,5,7,12,14,17,18	4,6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,5,7,12,14,16	4,6,8,9,13,15	2^{-1}

Table 0.1278 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,5,7,17	4,6,8,9,11,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,5,7,16,18	4,6,8,9,11,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,5,7,17,18	4,6,8,9,11,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,5,7,16	4,6,8,9,11,15	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,5,7,14,18	4,6,8,9,11,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,5,7,14,16,17	4,6,8,9,11,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,5,7,14	4,6,8,9,11,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,5,7,14,16,17,18	4,6,8,9,11,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,5,7,17,18	4,6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,5,7,16	4,6,8,9,11,13	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,17	4,6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,5,7,16,18	4,6,8,9,11,13,15,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,5,7,14	4,6,8,9,11,13	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,5,7,14,16,17,18	4,6,8,9,11,13,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,5,7,14,18	4,6,8,9,11,13,15,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,5,7,14,16,17	4,6,8,9,11,13,15,17	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,5,7,12,18	4,6,8,9,11,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,12,16,17	4,6,8,9,11,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,5,7,12	4,6,8,9,11,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,12,16,17,18	4,6,8,9,11,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,12,14,17	4,6,8,9,11,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,12,14,16,18	4,6,8,9,11,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,12,14,17,18	4,6,8,9,11,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,12,14,16	4,6,8,9,11,15	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,5,7,12	4,6,8,9,11,13	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,5,7,12,16,17,18	4,6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,5,7,12,18	4,6,8,9,11,13,15,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,5,7,12,16,17	4,6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,5,7,12,14,17,18	4,6,8,9,11,13,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,12,14,16	4,6,8,9,11,13	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,5,7,12,14,17	4,6,8,9,11,13,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,12,14,16,18	4,6,8,9,11,13,15,18	2^{-12}

Table 0.1279 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,5,7,10	4,6,8,9	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,5,7,10,16,17,18	4,6,8,9,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,5,7,10,18	4,6,8,9,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,5,7,10,16,17	4,6,8,9,15,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,5,7,10,14,17,18	4,6,8,9,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,10,14,16	4,6,8,9	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,5,7,10,14,17	4,6,8,9,15,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,5,7,10,14,16,18	4,6,8,9,15,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,5,7,10,18	4,6,8,9,13,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,5,7,10,16,17	4,6,8,9,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,5,7,10	4,6,8,9,13,15	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,5,7,10,16,17,18	4,6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,5,7,10,14,17	4,6,8,9,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,10,14,16,18	4,6,8,9,13,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,5,7,10,14,17,18	4,6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,10,14,16	4,6,8,9,13,15	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,10,12,17,18	4,6,8,9,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,10,12,16	4,6,8,9	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,10,12,17	4,6,8,9,15,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,10,12,16,18	4,6,8,9,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,5,7,10,12,14	4,6,8,9	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,10,12,14,16,17,18	4,6,8,9,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,5,7,10,12,14,18	4,6,8,9,15,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,10,12,14,16,17	4,6,8,9,15,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,10,12,17	4,6,8,9,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,10,12,16,18	4,6,8,9,13,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,10,12,17,18	4,6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,10,12,16	4,6,8,9,13,15	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,5,7,10,12,14,18	4,6,8,9,13,18	2^{-34}
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,10,12,14,16,17	4,6,8,9,13,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,5,7,10,12,14	4,6,8,9,13,15	2^{-34}
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,10,12,14,16,17,18	4,6,8,9,13,15,17,18	$2^{-17.5}$

Table 0.1280 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,5,7,10,18	4,6,8,9,11,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,5,7,10,16,17	4,6,8,9,11,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,5,7,10	4,6,8,9,11,15	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,5,7,10,16,17,18	4,6,8,9,11,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,10,14,17	4,6,8,9,11,17	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,10,14,16,18	4,6,8,9,11,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,10,14,17,18	4,6,8,9,11,15,17,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,10,14,16	4,6,8,9,11,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,5,7,10	4,6,8,9,11,13	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,7,10,16,17,18	4,6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,5,7,10,18	4,6,8,9,11,13,15,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,7,10,16,17	4,6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,5,7,10,14,17,18	4,6,8,9,11,13,17,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,5,7,10,14,16	4,6,8,9,11,13	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,5,7,10,14,17	4,6,8,9,11,13,15,17	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,5,7,10,14,16,18	4,6,8,9,11,13,15,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,5,7,10,12,17	4,6,8,9,11,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,10,12,16,18	4,6,8,9,11,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,5,7,10,12,17,18	4,6,8,9,11,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,10,12,16	4,6,8,9,11,15	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,7,10,12,14,18	4,6,8,9,11,18	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,5,7,10,12,14,16,17	4,6,8,9,11,17	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,7,10,12,14	4,6,8,9,11,15	$2^{-28.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,5,7,10,12,14,16,17,18	4,6,8,9,11,15,17,18	2^{-12}
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,5,7,10,12,17,18	4,6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,5,7,10,12,16	4,6,8,9,11,13	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,5,7,10,12,17	4,6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,5,7,10,12,16,18	4,6,8,9,11,13,15,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,10,12,14	4,6,8,9,11,13	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,5,7,10,12,14,16,17,18	4,6,8,9,11,13,17,18	$2^{-6.5}$
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,5,7,10,12,14,18	4,6,8,9,11,13,15,18	2^{-23}
$(1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,5,7,10,12,14,16,17	4,6,8,9,11,13,15,17	$2^{-6.5}$

Table 0.1281 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3	—	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,16,17,18	17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,18	15,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,16,17	15,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,14,17,18	17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,14,16	—	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,14,17	15,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,14,16,18	15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,18	13,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,16,17	13,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3	13,15	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,16,17,18	13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,14,17	13,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,14,16,18	13,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,14,17,18	13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,14,16	13,15	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,12,17,18	17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,12,16	—	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,12,17	15,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,12,16,18	15,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,12,14	—	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,12,14,16,17,18	17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,12,14,18	15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,12,14,16,17	15,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,12,17	13,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,12,16,18	13,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,12,17,18	13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,12,16	13,15	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,12,14,18	13,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,12,14,16,17	13,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,12,14	13,15	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,12,14,16,17,18	13,15,17,18	$2^{-28.5}$

Table 0.1282 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,18	11,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,16,17	11,17	2^{-34}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3	11,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,16,17,18	11,15,17,18	2^{-34}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,14,17	11,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,14,16,18	11,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,14,17,18	11,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,14,16	11,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3	11,13	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,16,17,18	11,13,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,18	11,13,15,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,16,17	11,13,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,14,17,18	11,13,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,14,16	11,13	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,14,17	11,13,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,14,16,18	11,13,15,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,12,17	11,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,12,16,18	11,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,12,17,18	11,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,12,16	11,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,12,14,18	11,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,12,14,16,17	11,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,12,14	11,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,12,14,16,17,18	11,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,12,17,18	11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,12,16	11,13	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,12,17	11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,12,16,18	11,13,15,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,12,14	11,13	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,12,14,16,17,18	11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,12,14,18	11,13,15,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,12,14,16,17	11,13,15,17	$2^{-17.5}$

Table 0.1283 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,10,17,18	17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,10,16	—	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,10,17	15,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,10,16,18	15,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,10,14	—	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,10,14,16,17,18	17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,10,14,18	15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,10,14,16,17	15,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,10,17	13,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,10,16,18	13,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,10,17,18	13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,10,16	13,15	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,10,14,18	13,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,10,14,16,17	13,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,10,14	13,15	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,10,14,16,17,18	13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,10,12	—	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,10,12,16,17,18	17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,10,12,18	15,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,10,12,16,17	15,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,10,12,14,17,18	17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,10,12,14,16	—	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,10,12,14,17	15,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,10,12,14,16,18	15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,10,12,18	13,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,10,12,16,17	13,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,10,12	13,15	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,10,12,16,17,18	13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,10,12,14,17	13,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,10,12,14,16,18	13,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,10,12,14,17,18	13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,10,12,14,16	13,15	2^{-12}

Table 0.1284 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,10,17	11,17	2^{-1}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,10,16,18	11,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,10,17,18	11,15,17,18	2^{-1}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,10,16	11,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,10,14,18	11,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,10,14,16,17	11,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,10,14	11,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,10,14,16,17,18	11,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,10,17,18	11,13,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,10,16	11,13	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,10,17	11,13,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,10,16,18	11,13,15,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,10,14	11,13	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,10,14,16,17,18	11,13,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,10,14,18	11,13,15,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,10,14,16,17	11,13,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,10,12,18	11,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,10,12,16,17	11,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,10,12	11,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,10,12,16,17,18	11,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,10,12,14,17	11,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,10,12,14,16,18	11,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,10,12,14,17,18	11,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,10,12,14,16	11,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,10,12	11,13	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,10,12,16,17,18	11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,10,12,18	11,13,15,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,10,12,16,17	11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,10,12,14,17,18	11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,10,12,14,16	11,13	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,10,12,14,17	11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,10,12,14,16,18	11,13,15,18	2^{-23}

Table 0.1285 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,18	9,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,16,17	9,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3	9,15	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,16,17,18	9,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,14,17	9,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,14,16,18	9,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,14,17,18	9,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,14,16	9,15	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3	9,13	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,16,17,18	9,13,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,18	9,13,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,16,17	9,13,15,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,14,17,18	9,13,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,14,16	9,13	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,14,17	9,13,15,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,14,16,18	9,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,12,17	9,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,12,16,18	9,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,12,17,18	9,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,12,16	9,15	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,12,14,18	9,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,12,14,16,17	9,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,12,14	9,15	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,12,14,16,17,18	9,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,12,17,18	9,13,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,12,16	9,13	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,12,17	9,13,15,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,12,16,18	9,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,12,14	9,13	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,12,14,16,17,18	9,13,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,12,14,18	9,13,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,12,14,16,17	9,13,15,17	2^{-12}

Table 0.1286 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3	9,11	2^{-1}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,16,17,18	9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,18	9,11,15,18	2^{-1}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,16,17	9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,14,17,18	9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,14,16	9,11	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,14,17	9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,14,16,18	9,11,15,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,18	9,11,13,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,16,17	9,11,13,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3	9,11,13,15	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,16,17,18	9,11,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,14,17	9,11,13,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,14,16,18	9,11,13,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,14,17,18	9,11,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,14,16	9,11,13,15	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,12,17,18	9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,12,16	9,11	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,12,17	9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,12,16,18	9,11,15,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,12,14	9,11	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,12,14,16,17,18	9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,12,14,18	9,11,15,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,12,14,16,17	9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,12,17	9,11,13,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,12,16,18	9,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,12,17,18	9,11,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,12,16	9,11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,12,14,18	9,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,12,14,16,17	9,11,13,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,12,14	9,11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,12,14,16,17,18	9,11,13,15,17,18	2^{-23}

Table 0.1287 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,10,17	9,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,10,16,18	9,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,10,17,18	9,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,10,16	9,15	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,10,14,18	9,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,10,14,16,17	9,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,10,14	9,15	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,10,14,16,17,18	9,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,10,17,18	9,13,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,10,16	9,13	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,10,17	9,13,15,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,10,16,18	9,13,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,10,14	9,13	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,10,14,16,17,18	9,13,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,10,14,18	9,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,10,14,16,17	9,13,15,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,10,12,18	9,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,10,12,16,17	9,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,10,12	9,15	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,10,12,16,17,18	9,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,10,12,14,17	9,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,10,12,14,16,18	9,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,10,12,14,17,18	9,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,10,12,14,16	9,15	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,10,12	9,13	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,10,12,16,17,18	9,13,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,10,12,18	9,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,10,12,16,17	9,13,15,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,10,12,14,17,18	9,13,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,10,12,14,16	9,13	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,10,12,14,17	9,13,15,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,10,12,14,16,18	9,13,15,18	$2^{-28.5}$

Table 0.1288 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,10,17,18	9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,10,16	9,11	2^{-34}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,10,17	9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,10,16,18	9,11,15,18	2^{-34}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,10,14	9,11	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,10,14,16,17,18	9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,10,14,18	9,11,15,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,10,14,16,17	9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,10,17	9,11,13,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,10,16,18	9,11,13,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,10,17,18	9,11,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,10,16	9,11,13,15	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,10,14,18	9,11,13,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,10,14,16,17	9,11,13,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,10,14	9,11,13,15	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,10,14,16,17,18	9,11,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,10,12	9,11	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,10,12,16,17,18	9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,10,12,18	9,11,15,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,10,12,16,17	9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,10,12,14,17,18	9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,10,12,14,16	9,11	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,10,12,14,17	9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,10,12,14,16,18	9,11,15,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,10,12,18	9,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,10,12,16,17	9,11,13,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,10,12	9,11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,10,12,16,17,18	9,11,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,10,12,14,17	9,11,13,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,10,12,14,16,18	9,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,10,12,14,17,18	9,11,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,10,12,14,16	9,11,13,15	$2^{-17.5}$

Table 0.1289 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,17,18	8,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,16	8	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,17	8,15,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,16,18	8,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,14	8	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,14,16,17,18	8,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,14,18	8,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,14,16,17	8,15,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,17	8,13,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,16,18	8,13,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,17,18	8,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,16	8,13,15	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,14,18	8,13,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,14,16,17	8,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,14	8,13,15	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,14,16,17,18	8,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,12	8	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,12,16,17,18	8,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,12,18	8,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,12,16,17	8,15,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,12,14,17,18	8,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,12,14,16	8	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,12,14,17	8,15,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,12,14,16,18	8,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,12,18	8,13,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,12,16,17	8,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,12	8,13,15	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,12,16,17,18	8,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,12,14,17	8,13,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,12,14,16,18	8,13,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,12,14,17,18	8,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,12,14,16	8,13,15	2^{-23}

Table 0.1290 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,17	8,11,17	2^{-34}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,16,18	8,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,17,18	8,11,15,17,18	2^{-34}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,16	8,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,14,18	8,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,14,16,17	8,11,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,14	8,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,14,16,17,18	8,11,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,17,18	8,11,13,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,16	8,11,13	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,17	8,11,13,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,16,18	8,11,13,15,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,14	8,11,13	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,14,16,17,18	8,11,13,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,14,18	8,11,13,15,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,14,16,17	8,11,13,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,12,18	8,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,12,16,17	8,11,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,12	8,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,12,16,17,18	8,11,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,12,14,17	8,11,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,12,14,16,18	8,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,12,14,17,18	8,11,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,12,14,16	8,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,12	8,11,13	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,12,16,17,18	8,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,12,18	8,11,13,15,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,12,16,17	8,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,12,14,17,18	8,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,12,14,16	8,11,13	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,12,14,17	8,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,12,14,16,18	8,11,13,15,18	2^{-12}

Table 0.1291 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,10	8	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,10,16,17,18	8,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,10,18	8,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,10,16,17	8,15,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,10,14,17,18	8,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,10,14,16	8	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,10,14,17	8,15,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,10,14,16,18	8,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,10,18	8,13,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,10,16,17	8,13,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,10	8,13,15	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,10,16,17,18	8,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,10,14,17	8,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,10,14,16,18	8,13,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,10,14,17,18	8,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,10,14,16	8,13,15	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,10,12,17,18	8,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,10,12,16	8	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,10,12,17	8,15,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,10,12,16,18	8,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,10,12,14	8	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,10,12,14,16,17,18	8,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,10,12,14,18	8,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,10,12,14,16,17	8,15,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,10,12,17	8,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,10,12,16,18	8,13,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,10,12,17,18	8,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,10,12,16	8,13,15	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,10,12,14,18	8,13,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,10,12,14,16,17	8,13,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,10,12,14	8,13,15	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,10,12,14,16,17,18	8,13,15,17,18	$2^{-6.5}$

Table 0.1292 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,10,18	8,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,10,16,17	8,11,17	2^{-1}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,10	8,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,10,16,17,18	8,11,15,17,18	2^{-1}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,10,14,17	8,11,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,10,14,16,18	8,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,10,14,17,18	8,11,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,10,14,16	8,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,10	8,11,13	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,10,16,17,18	8,11,13,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,10,18	8,11,13,15,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,10,16,17	8,11,13,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,10,14,17,18	8,11,13,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,10,14,16	8,11,13	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,10,14,17	8,11,13,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,10,14,16,18	8,11,13,15,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,10,12,17	8,11,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,10,12,16,18	8,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,10,12,17,18	8,11,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,10,12,16	8,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,10,12,14,18	8,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,10,12,14,16,17	8,11,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,10,12,14	8,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,10,12,14,16,17,18	8,11,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,10,12,17,18	8,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,10,12,16	8,11,13	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,10,12,17	8,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,10,12,16,18	8,11,13,15,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,10,12,14	8,11,13	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,10,12,14,16,17,18	8,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,10,12,14,18	8,11,13,15,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,10,12,14,16,17	8,11,13,15,17	$2^{-17.5}$

Table 0.1293 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,17	8,9,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,16,18	8,9,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,17,18	8,9,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,16	8,9,15	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,14,18	8,9,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,14,16,17	8,9,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,14	8,9,15	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,14,16,17,18	8,9,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,17,18	8,9,13,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,16	8,9,13	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,17	8,9,13,15,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,16,18	8,9,13,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,14	8,9,13	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,14,16,17,18	8,9,13,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,14,18	8,9,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,14,16,17	8,9,13,15,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,12,18	8,9,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,12,16,17	8,9,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,12	8,9,15	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,12,16,17,18	8,9,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,12,14,17	8,9,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,12,14,16,18	8,9,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,12,14,17,18	8,9,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,12,14,16	8,9,15	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,12	8,9,13	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,12,16,17,18	8,9,13,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,12,18	8,9,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,12,16,17	8,9,13,15,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,12,14,17,18	8,9,13,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,12,14,16	8,9,13	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,12,14,17	8,9,13,15,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,12,14,16,18	8,9,13,15,18	$2^{-6.5}$

Table 0.1294 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,17,18	8,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,16	8,9,11	2^{-1}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,17	8,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,16,18	8,9,11,15,18	2^{-1}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,14	8,9,11	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,14,16,17,18	8,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,14,18	8,9,11,15,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,14,16,17	8,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,17	8,9,11,13,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,16,18	8,9,11,13,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,17,18	8,9,11,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,16	8,9,11,13,15	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,14,18	8,9,11,13,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,14,16,17	8,9,11,13,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,14	8,9,11,13,15	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,14,16,17,18	8,9,11,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,12	8,9,11	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,12,16,17,18	8,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,12,18	8,9,11,15,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,12,16,17	8,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,12,14,17,18	8,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,12,14,16	8,9,11	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,12,14,17	8,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,12,14,16,18	8,9,11,15,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,12,18	8,9,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,12,16,17	8,9,11,13,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,12	8,9,11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,12,16,17,18	8,9,11,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,12,14,17	8,9,11,13,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,12,14,16,18	8,9,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,12,14,17,18	8,9,11,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,12,14,16	8,9,11,13,15	$2^{-17.5}$

Table 0.1295 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,10,18	8,9,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,10,16,17	8,9,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,10	8,9,15	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,10,16,17,18	8,9,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,10,14,17	8,9,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,10,14,16,18	8,9,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,10,14,17,18	8,9,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,10,14,16	8,9,15	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,10	8,9,13	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,10,16,17,18	8,9,13,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,10,18	8,9,13,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,10,16,17	8,9,13,15,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,10,14,17,18	8,9,13,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,10,14,16	8,9,13	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,10,14,17	8,9,13,15,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,10,14,16,18	8,9,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,10,12,17	8,9,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,10,12,16,18	8,9,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,10,12,17,18	8,9,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,10,12,16	8,9,15	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,10,12,14,18	8,9,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,10,12,14,16,17	8,9,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,10,12,14	8,9,15	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,10,12,14,16,17,18	8,9,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,10,12,17,18	8,9,13,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,10,12,16	8,9,13	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,10,12,17	8,9,13,15,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,10,12,16,18	8,9,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,10,12,14	8,9,13	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,10,12,14,16,17,18	8,9,13,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,10,12,14,18	8,9,13,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,10,12,14,16,17	8,9,13,15,17	2^{-23}

Table 0.1296 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,10	8,9,11	2^{-34}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,10,16,17,18	8,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,10,18	8,9,11,15,18	2^{-34}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,10,16,17	8,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,10,14,17,18	8,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,10,14,16	8,9,11	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,10,14,17	8,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,10,14,16,18	8,9,11,15,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,10,18	8,9,11,13,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,10,16,17	8,9,11,13,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,10	8,9,11,13,15	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,10,16,17,18	8,9,11,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,10,14,17	8,9,11,13,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,10,14,16,18	8,9,11,13,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,10,14,17,18	8,9,11,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,10,14,16	8,9,11,13,15	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,10,12,17,18	8,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,10,12,16	8,9,11	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,10,12,17	8,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,10,12,16,18	8,9,11,15,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,10,12,14	8,9,11	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,10,12,14,16,17,18	8,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,10,12,14,18	8,9,11,15,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,10,12,14,16,17	8,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,10,12,17	8,9,11,13,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,10,12,16,18	8,9,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,10,12,17,18	8,9,11,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,10,12,16	8,9,11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,10,12,14,18	8,9,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,10,12,14,16,17	8,9,11,13,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,10,12,14	8,9,11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,10,12,14,16,17,18	8,9,11,13,15,17,18	2^{-12}

Table 0.1297 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,7,18	18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,7,16,17	17	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,7	15	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,7,16,17,18	15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,7,14,17	17	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,7,14,16,18	18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,7,14,17,18	15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,7,14,16	15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,7	13	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,7,16,17,18	13,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,7,18	13,15,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,7,16,17	13,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,7,14,17,18	13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,7,14,16	13	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,7,14,17	13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,7,14,16,18	13,15,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,7,12,17	17	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,7,12,16,18	18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,7,12,17,18	15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,7,12,16	15	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,7,12,14,18	18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,7,12,14,16,17	17	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,7,12,14	15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,7,12,14,16,17,18	15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,7,12,17,18	13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,7,12,16	13	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,7,12,17	13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,7,12,16,18	13,15,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,7,12,14	13	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,7,12,14,16,17,18	13,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,7,12,14,18	13,15,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,7,12,14,16,17	13,15,17	$2^{-28.5}$

Table 0.1298 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,7	11	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,7,16,17,18	11,17,18	2^{-34}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,7,18	11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,7,16,17	11,15,17	2^{-34}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,7,14,17,18	11,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,7,14,16	11	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,7,14,17	11,15,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,7,14,16,18	11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,7,18	11,13,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,7,16,17	11,13,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,7	11,13,15	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,7,16,17,18	11,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,7,14,17	11,13,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,7,14,16,18	11,13,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,7,14,17,18	11,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,7,14,16	11,13,15	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,7,12,17,18	11,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,7,12,16	11	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,7,12,17	11,15,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,7,12,16,18	11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,7,12,14	11	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,7,12,14,16,17,18	11,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,7,12,14,18	11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,7,12,14,16,17	11,15,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,7,12,17	11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,7,12,16,18	11,13,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,7,12,17,18	11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,7,12,16	11,13,15	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,7,12,14,18	11,13,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,7,12,14,16,17	11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,7,12,14	11,13,15	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,7,12,14,16,17,18	11,13,15,17,18	$2^{-17.5}$

Table 0.1299 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,7,10,17	17	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,7,10,16,18	18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,7,10,17,18	15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,7,10,16	15	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,7,10,14,18	18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,7,10,14,16,17	17	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,7,10,14	15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,7,10,14,16,17,18	15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,7,10,17,18	13,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,7,10,16	13	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,7,10,17	13,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,7,10,16,18	13,15,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,7,10,14	13	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,7,10,14,16,17,18	13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,7,10,14,18	13,15,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,7,10,14,16,17	13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,7,10,12,18	18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,7,10,12,16,17	17	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,7,10,12	15	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,7,10,12,16,17,18	15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,7,10,12,14,17	17	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,7,10,12,14,16,18	18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,7,10,12,14,17,18	15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,7,10,12,14,16	15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,7,10,12	13	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,7,10,12,16,17,18	13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,7,10,12,18	13,15,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,7,10,12,16,17	13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,7,10,12,14,17,18	13,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,7,10,12,14,16	13	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,7,10,12,14,17	13,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,7,10,12,14,16,18	13,15,18	2^{-12}

Table 0.1300 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,7,10,17,18	11,17,18	2^{-1}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,7,10,16	11	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,7,10,17	11,15,17	2^{-1}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,7,10,16,18	11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,7,10,14	11	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,7,10,14,16,17,18	11,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,7,10,14,18	11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,7,10,14,16,17	11,15,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,7,10,17	11,13,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,7,10,16,18	11,13,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,7,10,17,18	11,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,7,10,16	11,13,15	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,7,10,14,18	11,13,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,7,10,14,16,17	11,13,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,7,10,14	11,13,15	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,7,10,14,16,17,18	11,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,7,10,12	11	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,7,10,12,16,17,18	11,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,7,10,12,18	11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,7,10,12,16,17	11,15,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,7,10,12,14,17,18	11,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,7,10,12,14,16	11	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,7,10,12,14,17	11,15,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,7,10,12,14,16,18	11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,7,10,12,18	11,13,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,7,10,12,16,17	11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,7,10,12	11,13,15	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,7,10,12,16,17,18	11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,7,10,12,14,17	11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,7,10,12,14,16,18	11,13,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,7,10,12,14,17,18	11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,7,10,12,14,16	11,13,15	2^{-23}

Table 0.1301 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,7	9	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,7,16,17,18	9,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,7,18	9,15,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,7,16,17	9,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,7,14,17,18	9,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,7,14,16	9	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,7,14,17	9,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,7,14,16,18	9,15,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,7,18	9,13,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,7,16,17	9,13,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,7	9,13,15	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,7,16,17,18	9,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,7,14,17	9,13,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,7,14,16,18	9,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,7,14,17,18	9,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,7,14,16	9,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,7,12,17,18	9,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,7,12,16	9	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,7,12,17	9,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,7,12,16,18	9,15,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,7,12,14	9	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,7,12,14,16,17,18	9,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,7,12,14,18	9,15,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,7,12,14,16,17	9,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,7,12,17	9,13,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,7,12,16,18	9,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,7,12,17,18	9,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,7,12,16	9,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,7,12,14,18	9,13,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,7,12,14,16,17	9,13,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,7,12,14	9,13,15	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,7,12,14,16,17,18	9,13,15,17,18	2^{-12}

Table 0.1302 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,7,18	9,11,18	2^{-1}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,7,16,17	9,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,7	9,11,15	2^{-1}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,7,16,17,18	9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,7,14,17	9,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,7,14,16,18	9,11,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,7,14,17,18	9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,7,14,16	9,11,15	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,7	9,11,13	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,7,16,17,18	9,11,13,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,7,18	9,11,13,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,7,16,17	9,11,13,15,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,7,14,17,18	9,11,13,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,7,14,16	9,11,13	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,7,14,17	9,11,13,15,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,7,14,16,18	9,11,13,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,7,12,17	9,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,7,12,16,18	9,11,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,7,12,17,18	9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,7,12,16	9,11,15	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,7,12,14,18	9,11,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,7,12,14,16,17	9,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,7,12,14	9,11,15	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,7,12,14,16,17,18	9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,7,12,17,18	9,11,13,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,7,12,16	9,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,7,12,17	9,11,13,15,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,7,12,16,18	9,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,7,12,14	9,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,7,12,14,16,17,18	9,11,13,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,7,12,14,18	9,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,7,12,14,16,17	9,11,13,15,17	2^{-23}

Table 0.1303 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,7,10,17,18	9,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,7,10,16	9	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,7,10,17	9,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,7,10,16,18	9,15,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,7,10,14	9	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,7,10,14,16,17,18	9,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,7,10,14,18	9,15,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,7,10,14,16,17	9,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,10,17	9,13,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,7,10,16,18	9,13,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,10,17,18	9,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,7,10,16	9,13,15	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,7,10,14,18	9,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,7,10,14,16,17	9,13,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,7,10,14	9,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,7,10,14,16,17,18	9,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,7,10,12	9	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,7,10,12,16,17,18	9,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,7,10,12,18	9,15,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,7,10,12,16,17	9,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,7,10,12,14,17,18	9,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,7,10,12,14,16	9	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,7,10,12,14,17	9,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,7,10,12,14,16,18	9,15,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,7,10,12,18	9,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,7,10,12,16,17	9,13,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,7,10,12	9,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,7,10,12,16,17,18	9,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,7,10,12,14,17	9,13,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,7,10,12,14,16,18	9,13,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,7,10,12,14,17,18	9,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,7,10,12,14,16	9,13,15	$2^{-28.5}$

Table 0.1304 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,7,10,17	9,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,7,10,16,18	9,11,18	2^{-34}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,7,10,17,18	9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,7,10,16	9,11,15	2^{-34}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,7,10,14,18	9,11,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,7,10,14,16,17	9,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,7,10,14	9,11,15	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,7,10,14,16,17,18	9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,7,10,17,18	9,11,13,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,7,10,16	9,11,13	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,7,10,17	9,11,13,15,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,7,10,16,18	9,11,13,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,7,10,14	9,11,13	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,7,10,14,16,17,18	9,11,13,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,7,10,14,18	9,11,13,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,7,10,14,16,17	9,11,13,15,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,7,10,12,18	9,11,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,7,10,12,16,17	9,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,7,10,12	9,11,15	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,7,10,12,16,17,18	9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,7,10,12,14,17	9,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,7,10,12,14,16,18	9,11,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,7,10,12,14,17,18	9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,7,10,12,14,16	9,11,15	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,7,10,12	9,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,7,10,12,16,17,18	9,11,13,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,7,10,12,18	9,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,7,10,12,16,17	9,11,13,15,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,7,10,12,14,17,18	9,11,13,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,7,10,12,14,16	9,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,7,10,12,14,17	9,11,13,15,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,7,10,12,14,16,18	9,11,13,15,18	$2^{-17.5}$

Table 0.1305 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,7,17	8,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,7,16,18	8,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,7,17,18	8,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,7,16	8,15	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,7,14,18	8,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,7,14,16,17	8,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,7,14	8,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,7,14,16,17,18	8,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,7,17,18	8,13,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,16	8,13	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,7,17	8,13,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,16,18	8,13,15,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,7,14	8,13	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,7,14,16,17,18	8,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,7,14,18	8,13,15,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,7,14,16,17	8,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,7,12,18	8,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,7,12,16,17	8,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,7,12	8,15	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,7,12,16,17,18	8,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,7,12,14,17	8,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,7,12,14,16,18	8,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,7,12,14,17,18	8,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,7,12,14,16	8,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,7,12	8,13	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,7,12,16,17,18	8,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,7,12,18	8,13,15,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,7,12,16,17	8,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,7,12,14,17,18	8,13,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,7,12,14,16	8,13	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,7,12,14,17	8,13,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,7,12,14,16,18	8,13,15,18	2^{-23}

Table 0.1306 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,7,17,18	8,11,17,18	2^{-34}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,7,16	8,11	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,7,17	8,11,15,17	2^{-34}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,7,16,18	8,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,7,14	8,11	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,7,14,16,17,18	8,11,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,7,14,18	8,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,7,14,16,17	8,11,15,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,7,17	8,11,13,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,7,16,18	8,11,13,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,7,17,18	8,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,7,16	8,11,13,15	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,7,14,18	8,11,13,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,7,14,16,17	8,11,13,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,7,14	8,11,13,15	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,7,14,16,17,18	8,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,7,12	8,11	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,7,12,16,17,18	8,11,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,7,12,18	8,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,7,12,16,17	8,11,15,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,7,12,14,17,18	8,11,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,7,12,14,16	8,11	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,7,12,14,17	8,11,15,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,7,12,14,16,18	8,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,7,12,18	8,11,13,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,7,12,16,17	8,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,7,12	8,11,13,15	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,7,12,16,17,18	8,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,7,12,14,17	8,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,7,12,14,16,18	8,11,13,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,7,12,14,17,18	8,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,7,12,14,16	8,11,13,15	2^{-12}

Table 0.1307 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,7,10,18	8,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,7,10,16,17	8,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,7,10	8,15	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,7,10,16,17,18	8,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,7,10,14,17	8,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,7,10,14,16,18	8,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,7,10,14,17,18	8,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,7,10,14,16	8,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,7,10	8,13	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,7,10,16,17,18	8,13,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,7,10,18	8,13,15,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,7,10,16,17	8,13,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,7,10,14,17,18	8,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,7,10,14,16	8,13	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,7,10,14,17	8,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,7,10,14,16,18	8,13,15,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,7,10,12,17	8,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,7,10,12,16,18	8,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,7,10,12,17,18	8,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,7,10,12,16	8,15	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,7,10,12,14,18	8,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,7,10,12,14,16,17	8,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,7,10,12,14	8,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,7,10,12,14,16,17,18	8,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,7,10,12,17,18	8,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,7,10,12,16	8,13	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,7,10,12,17	8,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,7,10,12,16,18	8,13,15,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,7,10,12,14	8,13	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,7,10,12,14,16,17,18	8,13,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,7,10,12,14,18	8,13,15,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,7,10,12,14,16,17	8,13,15,17	$2^{-6.5}$

Table 0.1308 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,7,10	8,11	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,7,10,16,17,18	8,11,17,18	2^{-1}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,7,10,18	8,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,7,10,16,17	8,11,15,17	2^{-1}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,7,10,14,17,18	8,11,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,7,10,14,16	8,11	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,7,10,14,17	8,11,15,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,7,10,14,16,18	8,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,7,10,18	8,11,13,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,7,10,16,17	8,11,13,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,7,10	8,11,13,15	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,7,10,16,17,18	8,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,7,10,14,17	8,11,13,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,7,10,14,16,18	8,11,13,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,7,10,14,17,18	8,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,7,10,14,16	8,11,13,15	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,7,10,12,17,18	8,11,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,7,10,12,16	8,11	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,7,10,12,17	8,11,15,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,7,10,12,16,18	8,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,7,10,12,14	8,11	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,7,10,12,14,16,17,18	8,11,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,7,10,12,14,18	8,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,7,10,12,14,16,17	8,11,15,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,7,10,12,17	8,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,7,10,12,16,18	8,11,13,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,7,10,12,17,18	8,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,7,10,12,16	8,11,13,15	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,7,10,12,14,18	8,11,13,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,7,10,12,14,16,17	8,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,7,10,12,14	8,11,13,15	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,7,10,12,14,16,17,18	8,11,13,15,17,18	$2^{-17.5}$

Table 0.1309 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,7,17,18	8,9,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,7,16	8,9	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,7,17	8,9,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,7,16,18	8,9,15,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,7,14	8,9	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,7,14,16,17,18	8,9,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,7,14,18	8,9,15,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,7,14,16,17	8,9,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,7,17	8,9,13,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,7,16,18	8,9,13,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,7,17,18	8,9,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,7,16	8,9,13,15	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,7,14,18	8,9,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,7,14,16,17	8,9,13,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,7,14	8,9,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,7,14,16,17,18	8,9,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,7,12	8,9	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,7,12,16,17,18	8,9,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,7,12,18	8,9,15,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,7,12,16,17	8,9,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,7,12,14,17,18	8,9,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,7,12,14,16	8,9	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,7,12,14,17	8,9,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,7,12,14,16,18	8,9,15,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,7,12,18	8,9,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,7,12,16,17	8,9,13,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,7,12	8,9,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,7,12,16,17,18	8,9,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,7,12,14,17	8,9,13,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,7,12,14,16,18	8,9,13,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,7,12,14,17,18	8,9,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,7,12,14,16	8,9,13,15	$2^{-6.5}$

Table 0.1310 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,7,17	8,9,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,7,16,18	8,9,11,18	2^{-1}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,7,17,18	8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,7,16	8,9,11,15	2^{-1}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,7,14,18	8,9,11,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,7,14,16,17	8,9,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,7,14	8,9,11,15	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,7,14,16,17,18	8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,7,17,18	8,9,11,13,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,7,16	8,9,11,13	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,7,17	8,9,11,13,15,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,7,16,18	8,9,11,13,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,7,14	8,9,11,13	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,7,14,16,17,18	8,9,11,13,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,7,14,18	8,9,11,13,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,7,14,16,17	8,9,11,13,15,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,7,12,18	8,9,11,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,7,12,16,17	8,9,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,7,12	8,9,11,15	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,7,12,16,17,18	8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,7,12,14,17	8,9,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,7,12,14,16,18	8,9,11,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,7,12,14,17,18	8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,7,12,14,16	8,9,11,15	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,7,12	8,9,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,7,12,16,17,18	8,9,11,13,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,7,12,18	8,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,7,12,16,17	8,9,11,13,15,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,7,12,14,17,18	8,9,11,13,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,7,12,14,16	8,9,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,7,12,14,17	8,9,11,13,15,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,7,12,14,16,18	8,9,11,13,15,18	$2^{-17.5}$

Table 0.1311 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,7,10	8,9	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,7,10,16,17,18	8,9,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,7,10,18	8,9,15,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,7,10,16,17	8,9,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,7,10,14,17,18	8,9,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,7,10,14,16	8,9	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,7,10,14,17	8,9,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,7,10,14,16,18	8,9,15,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,7,10,18	8,9,13,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,7,10,16,17	8,9,13,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,7,10	8,9,13,15	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,7,10,16,17,18	8,9,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,7,10,14,17	8,9,13,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,7,10,14,16,18	8,9,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,7,10,14,17,18	8,9,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,7,10,14,16	8,9,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,7,10,12,17,18	8,9,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,7,10,12,16	8,9	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,7,10,12,17	8,9,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,7,10,12,16,18	8,9,15,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,7,10,12,14	8,9	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,7,10,12,14,16,17,18	8,9,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,7,10,12,14,18	8,9,15,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,7,10,12,14,16,17	8,9,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,7,10,12,17	8,9,13,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,7,10,12,16,18	8,9,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,7,10,12,17,18	8,9,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,7,10,12,16	8,9,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,7,10,12,14,18	8,9,13,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,7,10,12,14,16,17	8,9,13,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,7,10,12,14	8,9,13,15	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,7,10,12,14,16,17,18	8,9,13,15,17,18	2^{-23}

Table 0.1312 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,7,10,18	8,9,11,18	2^{-34}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,7,10,16,17	8,9,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,7,10	8,9,11,15	2^{-34}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,7,10,16,17,18	8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,7,10,14,17	8,9,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,7,10,14,16,18	8,9,11,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,7,10,14,17,18	8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,7,10,14,16	8,9,11,15	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,7,10	8,9,11,13	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,7,10,16,17,18	8,9,11,13,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,7,10,18	8,9,11,13,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,7,10,16,17	8,9,11,13,15,17	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,7,10,14,17,18	8,9,11,13,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,7,10,14,16	8,9,11,13	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,7,10,14,17	8,9,11,13,15,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,7,10,14,16,18	8,9,11,13,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,7,10,12,17	8,9,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,7,10,12,16,18	8,9,11,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,7,10,12,17,18	8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,7,10,12,16	8,9,11,15	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,7,10,12,14,18	8,9,11,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,7,10,12,14,16,17	8,9,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,7,10,12,14	8,9,11,15	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,7,10,12,14,16,17,18	8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,7,10,12,17,18	8,9,11,13,17,18	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,7,10,12,16	8,9,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,7,10,12,17	8,9,11,13,15,17	2^{-23}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,7,10,12,16,18	8,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,7,10,12,14	8,9,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,7,10,12,14,16,17,18	8,9,11,13,17,18	2^{-12}
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,7,10,12,14,18	8,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,7,10,12,14,16,17	8,9,11,13,15,17	2^{-12}

Table 0.1313 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,17,18	6,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,16	6	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,17	6,15,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,16,18	6,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,14	6	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,14,16,17,18	6,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,14,18	6,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,14,16,17	6,15,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,17	6,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,16,18	6,13,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,17,18	6,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,16	6,13,15	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,14,18	6,13,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,14,16,17	6,13,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,14	6,13,15	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,14,16,17,18	6,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,12	6	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,12,16,17,18	6,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,12,18	6,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,12,16,17	6,15,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,12,14,17,18	6,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,12,14,16	6	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,12,14,17	6,15,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,12,14,16,18	6,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,12,18	6,13,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,12,16,17	6,13,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,12	6,13,15	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,12,16,17,18	6,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,12,14,17	6,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,12,14,16,18	6,13,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,12,14,17,18	6,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,12,14,16	6,13,15	2^{-23}

Table 0.1314 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,17	6,11,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,16,18	6,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,17,18	6,11,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,16	6,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,14,18	6,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,14,16,17	6,11,17	2^{-34}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,14	6,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,14,16,17,18	6,11,15,17,18	2^{-34}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,17,18	6,11,13,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,16	6,11,13	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,17	6,11,13,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,16,18	6,11,13,15,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,14	6,11,13	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,14,16,17,18	6,11,13,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,14,18	6,11,13,15,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,14,16,17	6,11,13,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,12,18	6,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,12,16,17	6,11,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,12	6,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,12,16,17,18	6,11,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,12,14,17	6,11,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,12,14,16,18	6,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,12,14,17,18	6,11,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,12,14,16	6,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,12	6,11,13	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,12,16,17,18	6,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,12,18	6,11,13,15,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,12,16,17	6,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,12,14,17,18	6,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,12,14,16	6,11,13	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,12,14,17	6,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,12,14,16,18	6,11,13,15,18	2^{-23}

Table 0.1315 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,10	6	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,10,16,17,18	6,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,10,18	6,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,10,16,17	6,15,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,10,14,17,18	6,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,10,14,16	6	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,10,14,17	6,15,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,10,14,16,18	6,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,10,18	6,13,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,10,16,17	6,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,10	6,13,15	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,10,16,17,18	6,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,10,14,17	6,13,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,10,14,16,18	6,13,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,10,14,17,18	6,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,10,14,16	6,13,15	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,10,12,17,18	6,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,10,12,16	6	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,10,12,17	6,15,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,10,12,16,18	6,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,10,12,14	6	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,10,12,14,16,17,18	6,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,10,12,14,18	6,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,10,12,14,16,17	6,15,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,10,12,17	6,13,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,10,12,16,18	6,13,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,10,12,17,18	6,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,10,12,16	6,13,15	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,10,12,14,18	6,13,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,10,12,14,16,17	6,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,10,12,14	6,13,15	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,10,12,14,16,17,18	6,13,15,17,18	$2^{-17.5}$

Table 0.1316 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,10,18	6,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,10,16,17	6,11,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,10	6,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,10,16,17,18	6,11,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,10,14,17	6,11,17	2^{-1}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,10,14,16,18	6,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,10,14,17,18	6,11,15,17,18	2^{-1}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,10,14,16	6,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,10	6,11,13	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,10,16,17,18	6,11,13,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,10,18	6,11,13,15,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,10,16,17	6,11,13,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,10,14,17,18	6,11,13,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,10,14,16	6,11,13	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,10,14,17	6,11,13,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,10,14,16,18	6,11,13,15,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,10,12,17	6,11,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,10,12,16,18	6,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,10,12,17,18	6,11,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,10,12,16	6,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,10,12,14,18	6,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,10,12,14,16,17	6,11,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,10,12,14	6,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,10,12,14,16,17,18	6,11,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,10,12,17,18	6,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,10,12,16	6,11,13	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,10,12,17	6,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,10,12,16,18	6,11,13,15,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,10,12,14	6,11,13	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,10,12,14,16,17,18	6,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,10,12,14,18	6,11,13,15,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,10,12,14,16,17	6,11,13,15,17	$2^{-17.5}$

Table 0.1317 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,17	6,9,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,16,18	6,9,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,17,18	6,9,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,16	6,9,15	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,14,18	6,9,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,14,16,17	6,9,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,14	6,9,15	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,14,16,17,18	6,9,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,17,18	6,9,13,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,16	6,9,13	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,17	6,9,13,15,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,16,18	6,9,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,14	6,9,13	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,14,16,17,18	6,9,13,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,14,18	6,9,13,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,14,16,17	6,9,13,15,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,12,18	6,9,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,12,16,17	6,9,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,12	6,9,15	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,12,16,17,18	6,9,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,12,14,17	6,9,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,12,14,16,18	6,9,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,12,14,17,18	6,9,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,12,14,16	6,9,15	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,12	6,9,13	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,12,16,17,18	6,9,13,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,12,18	6,9,13,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,12,16,17	6,9,13,15,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,12,14,17,18	6,9,13,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,12,14,16	6,9,13	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,12,14,17	6,9,13,15,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,12,14,16,18	6,9,13,15,18	$2^{-17.5}$

Table 0.1318 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,17,18	6,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,16	6,9,11	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,17	6,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,16,18	6,9,11,15,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,14	6,9,11	2^{-1}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,14,16,17,18	6,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,14,18	6,9,11,15,18	2^{-1}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,14,16,17	6,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,17	6,9,11,13,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,16,18	6,9,11,13,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,17,18	6,9,11,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,16	6,9,11,13,15	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,14,18	6,9,11,13,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,14,16,17	6,9,11,13,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,14	6,9,11,13,15	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,14,16,17,18	6,9,11,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,12	6,9,11	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,12,16,17,18	6,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,12,18	6,9,11,15,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,12,16,17	6,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,12,14,17,18	6,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,12,14,16	6,9,11	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,12,14,17	6,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,12,14,16,18	6,9,11,15,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,12,18	6,9,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,12,16,17	6,9,11,13,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,12	6,9,11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,12,16,17,18	6,9,11,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,12,14,17	6,9,11,13,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,12,14,16,18	6,9,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,12,14,17,18	6,9,11,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,12,14,16	6,9,11,13,15	$2^{-17.5}$

Table 0.1319 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,10,18	6,9,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,10,16,17	6,9,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,10	6,9,15	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,10,16,17,18	6,9,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,10,14,17	6,9,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,10,14,16,18	6,9,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,10,14,17,18	6,9,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,10,14,16	6,9,15	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,10	6,9,13	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,10,16,17,18	6,9,13,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,10,18	6,9,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,10,16,17	6,9,13,15,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,10,14,17,18	6,9,13,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,10,14,16	6,9,13	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,10,14,17	6,9,13,15,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,10,14,16,18	6,9,13,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,10,12,17	6,9,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,10,12,16,18	6,9,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,10,12,17,18	6,9,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,10,12,16	6,9,15	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,10,12,14,18	6,9,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,10,12,14,16,17	6,9,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,10,12,14	6,9,15	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,10,12,14,16,17,18	6,9,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,10,12,17,18	6,9,13,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,10,12,16	6,9,13	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,10,12,17	6,9,13,15,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,10,12,16,18	6,9,13,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,10,12,14	6,9,13	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,10,12,14,16,17,18	6,9,13,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,10,12,14,18	6,9,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,10,12,14,16,17	6,9,13,15,17	2^{-23}

Table 0.1320 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,10	6,9,11	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,10,16,17,18	6,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,10,18	6,9,11,15,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,10,16,17	6,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,10,14,17,18	6,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,10,14,16	6,9,11	2^{-34}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,10,14,17	6,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,10,14,16,18	6,9,11,15,18	2^{-34}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,10,18	6,9,11,13,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,10,16,17	6,9,11,13,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,10	6,9,11,13,15	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,10,16,17,18	6,9,11,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,10,14,17	6,9,11,13,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,10,14,16,18	6,9,11,13,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,10,14,17,18	6,9,11,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,10,14,16	6,9,11,13,15	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,10,12,17,18	6,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,10,12,16	6,9,11	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,10,12,17	6,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,10,12,16,18	6,9,11,15,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,10,12,14	6,9,11	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,10,12,14,16,17,18	6,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,10,12,14,18	6,9,11,15,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,10,12,14,16,17	6,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,10,12,17	6,9,11,13,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,10,12,16,18	6,9,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,10,12,17,18	6,9,11,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,10,12,16	6,9,11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,10,12,14,18	6,9,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,10,12,14,16,17	6,9,11,13,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,10,12,14	6,9,11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,10,12,14,16,17,18	6,9,11,13,15,17,18	2^{-23}

Table 0.1321 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3	6,8	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,16,17,18	6,8,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,18	6,8,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,16,17	6,8,15,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,14,17,18	6,8,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,14,16	6,8	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,14,17	6,8,15,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,14,16,18	6,8,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,18	6,8,13,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,16,17	6,8,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3	6,8,13,15	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,16,17,18	6,8,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,14,17	6,8,13,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,14,16,18	6,8,13,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,14,17,18	6,8,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,14,16	6,8,13,15	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,12,17,18	6,8,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,12,16	6,8	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,12,17	6,8,15,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,12,16,18	6,8,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,12,14	6,8	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,12,14,16,17,18	6,8,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,12,14,18	6,8,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,12,14,16,17	6,8,15,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,12,17	6,8,13,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,12,16,18	6,8,13,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,12,17,18	6,8,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,12,16	6,8,13,15	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,12,14,18	6,8,13,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,12,14,16,17	6,8,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,12,14	6,8,13,15	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,12,14,16,17,18	6,8,13,15,17,18	$2^{-17.5}$

Table 0.1322 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,18	6,8,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,16,17	6,8,11,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3	6,8,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,16,17,18	6,8,11,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,14,17	6,8,11,17	2^{-34}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,14,16,18	6,8,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,14,17,18	6,8,11,15,17,18	2^{-34}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,14,16	6,8,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3	6,8,11,13	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,16,17,18	6,8,11,13,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,18	6,8,11,13,15,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,16,17	6,8,11,13,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,14,17,18	6,8,11,13,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,14,16	6,8,11,13	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,14,17	6,8,11,13,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,14,16,18	6,8,11,13,15,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,12,17	6,8,11,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,12,16,18	6,8,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,12,17,18	6,8,11,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,12,16	6,8,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,12,14,18	6,8,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,12,14,16,17	6,8,11,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,12,14	6,8,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,12,14,16,17,18	6,8,11,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,12,17,18	6,8,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,12,16	6,8,11,13	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,12,17	6,8,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,12,16,18	6,8,11,13,15,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,12,14	6,8,11,13	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,12,14,16,17,18	6,8,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,12,14,18	6,8,11,13,15,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,12,14,16,17	6,8,11,13,15,17	$2^{-17.5}$

Table 0.1323 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,10,17,18	6,8,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,10,16	6,8	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,10,17	6,8,15,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,10,16,18	6,8,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,10,14	6,8	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,10,14,16,17,18	6,8,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,10,14,18	6,8,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,10,14,16,17	6,8,15,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,10,17	6,8,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,10,16,18	6,8,13,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,10,17,18	6,8,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,10,16	6,8,13,15	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,10,14,18	6,8,13,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,10,14,16,17	6,8,13,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,10,14	6,8,13,15	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,10,14,16,17,18	6,8,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,10,12	6,8	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,10,12,16,17,18	6,8,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,10,12,18	6,8,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,10,12,16,17	6,8,15,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,10,12,14,17,18	6,8,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,10,12,14,16	6,8	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,10,12,14,17	6,8,15,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,10,12,14,16,18	6,8,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,10,12,18	6,8,13,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,10,12,16,17	6,8,13,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,10,12	6,8,13,15	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,10,12,16,17,18	6,8,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,10,12,14,17	6,8,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,10,12,14,16,18	6,8,13,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,10,12,14,17,18	6,8,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,10,12,14,16	6,8,13,15	2^{-12}

Table 0.1324 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,10,17	6,8,11,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,10,16,18	6,8,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,10,17,18	6,8,11,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,10,16	6,8,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,10,14,18	6,8,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,10,14,16,17	6,8,11,17	2^{-1}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,10,14	6,8,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,10,14,16,17,18	6,8,11,15,17,18	2^{-1}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,10,17,18	6,8,11,13,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,10,16	6,8,11,13	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,10,17	6,8,11,13,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,10,16,18	6,8,11,13,15,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,10,14	6,8,11,13	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,10,14,16,17,18	6,8,11,13,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,10,14,18	6,8,11,13,15,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,10,14,16,17	6,8,11,13,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,10,12,18	6,8,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,10,12,16,17	6,8,11,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,10,12	6,8,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,10,12,16,17,18	6,8,11,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,10,12,14,17	6,8,11,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,10,12,14,16,18	6,8,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,10,12,14,17,18	6,8,11,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,10,12,14,16	6,8,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,10,12	6,8,11,13	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,10,12,16,17,18	6,8,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,10,12,18	6,8,11,13,15,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,10,12,16,17	6,8,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,10,12,14,17,18	6,8,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,10,12,14,16	6,8,11,13	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,10,12,14,17	6,8,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,10,12,14,16,18	6,8,11,13,15,18	2^{-12}

Table 0.1325 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,18	6,8,9,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,16,17	6,8,9,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3	6,8,9,15	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,16,17,18	6,8,9,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,14,17	6,8,9,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,14,16,18	6,8,9,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,14,17,18	6,8,9,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,14,16	6,8,9,15	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3	6,8,9,13	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,16,17,18	6,8,9,13,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,18	6,8,9,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,16,17	6,8,9,13,15,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,14,17,18	6,8,9,13,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,14,16	6,8,9,13	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,14,17	6,8,9,13,15,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,14,16,18	6,8,9,13,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,12,17	6,8,9,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,12,16,18	6,8,9,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,12,17,18	6,8,9,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,12,16	6,8,9,15	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,12,14,18	6,8,9,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,12,14,16,17	6,8,9,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,12,14	6,8,9,15	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,12,14,16,17,18	6,8,9,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,12,17,18	6,8,9,13,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,12,16	6,8,9,13	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,12,17	6,8,9,13,15,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,12,16,18	6,8,9,13,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,12,14	6,8,9,13	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,12,14,16,17,18	6,8,9,13,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,12,14,18	6,8,9,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,12,14,16,17	6,8,9,13,15,17	2^{-12}

Table 0.1326 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3	6,8,9,11	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,16,17,18	6,8,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,18	6,8,9,11,15,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,16,17	6,8,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,14,17,18	6,8,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,14,16	6,8,9,11	2^{-1}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,14,17	6,8,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,14,16,18	6,8,9,11,15,18	2^{-1}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,18	6,8,9,11,13,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,16,17	6,8,9,11,13,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3	6,8,9,11,13,15	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,16,17,18	6,8,9,11,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,14,17	6,8,9,11,13,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,14,16,18	6,8,9,11,13,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,14,17,18	6,8,9,11,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,14,16	6,8,9,11,13,15	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,12,17,18	6,8,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,12,16	6,8,9,11	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,12,17	6,8,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,12,16,18	6,8,9,11,15,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,12,14	6,8,9,11	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,12,14,16,17,18	6,8,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,12,14,18	6,8,9,11,15,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,12,14,16,17	6,8,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,12,17	6,8,9,11,13,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,12,16,18	6,8,9,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,12,17,18	6,8,9,11,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,12,16	6,8,9,11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,12,14,18	6,8,9,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,12,14,16,17	6,8,9,11,13,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,12,14	6,8,9,11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,12,14,16,17,18	6,8,9,11,13,15,17,18	2^{-12}

Table 0.1327 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,10,17	6,8,9,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,10,16,18	6,8,9,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,10,17,18	6,8,9,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,10,16	6,8,9,15	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,10,14,18	6,8,9,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,10,14,16,17	6,8,9,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,10,14	6,8,9,15	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,10,14,16,17,18	6,8,9,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,10,17,18	6,8,9,13,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,10,16	6,8,9,13	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,10,17	6,8,9,13,15,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,10,16,18	6,8,9,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,10,14	6,8,9,13	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,10,14,16,17,18	6,8,9,13,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,10,14,18	6,8,9,13,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,10,14,16,17	6,8,9,13,15,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,10,12,18	6,8,9,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,10,12,16,17	6,8,9,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,10,12	6,8,9,15	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,10,12,16,17,18	6,8,9,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,10,12,14,17	6,8,9,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,10,12,14,16,18	6,8,9,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,10,12,14,17,18	6,8,9,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,10,12,14,16	6,8,9,15	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,10,12	6,8,9,13	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,10,12,16,17,18	6,8,9,13,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,10,12,18	6,8,9,13,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,10,12,16,17	6,8,9,13,15,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,10,12,14,17,18	6,8,9,13,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,10,12,14,16	6,8,9,13	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,10,12,14,17	6,8,9,13,15,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,10,12,14,16,18	6,8,9,13,15,18	$2^{-17.5}$

Table 0.1328 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,10,17,18	6,8,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,10,16	6,8,9,11	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,10,17	6,8,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,10,16,18	6,8,9,11,15,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,10,14	6,8,9,11	2^{-34}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,10,14,16,17,18	6,8,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,10,14,18	6,8,9,11,15,18	2^{-34}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,10,14,16,17	6,8,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,10,17	6,8,9,11,13,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,10,16,18	6,8,9,11,13,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,10,17,18	6,8,9,11,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,10,16	6,8,9,11,13,15	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,10,14,18	6,8,9,11,13,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,10,14,16,17	6,8,9,11,13,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,10,14	6,8,9,11,13,15	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,10,14,16,17,18	6,8,9,11,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,10,12	6,8,9,11	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,10,12,16,17,18	6,8,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,10,12,18	6,8,9,11,15,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,10,12,16,17	6,8,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,10,12,14,17,18	6,8,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,10,12,14,16	6,8,9,11	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,10,12,14,17	6,8,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,10,12,14,16,18	6,8,9,11,15,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,10,12,18	6,8,9,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,10,12,16,17	6,8,9,11,13,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,10,12	6,8,9,11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,10,12,16,17,18	6,8,9,11,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,10,12,14,17	6,8,9,11,13,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,10,12,14,16,18	6,8,9,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,10,12,14,17,18	6,8,9,11,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,10,12,14,16	6,8,9,11,13,15	$2^{-17.5}$

Table 0.1329 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,7,17	6,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,7,16,18	6,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,7,17,18	6,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,7,16	6,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,7,14,18	6,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,7,14,16,17	6,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,7,14	6,15	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,7,14,16,17,18	6,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,7,17,18	6,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,7,16	6,13	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,7,17	6,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,7,16,18	6,13,15,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,7,14	6,13	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,7,14,16,17,18	6,13,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,7,14,18	6,13,15,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,7,14,16,17	6,13,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,7,12,18	6,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,7,12,16,17	6,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,7,12	6,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,7,12,16,17,18	6,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,7,12,14,17	6,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,7,12,14,16,18	6,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,7,12,14,17,18	6,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,7,12,14,16	6,15	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,7,12	6,13	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,7,12,16,17,18	6,13,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,7,12,18	6,13,15,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,7,12,16,17	6,13,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,7,12,14,17,18	6,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,7,12,14,16	6,13	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,7,12,14,17	6,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,7,12,14,16,18	6,13,15,18	2^{-23}

Table 0.1330 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,7,17,18	6,11,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,7,16	6,11	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,7,17	6,11,15,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,7,16,18	6,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,7,14	6,11	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,7,14,16,17,18	6,11,17,18	2^{-34}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,7,14,18	6,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,7,14,16,17	6,11,15,17	2^{-34}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,7,17	6,11,13,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,7,16,18	6,11,13,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,7,17,18	6,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,7,16	6,11,13,15	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,7,14,18	6,11,13,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,7,14,16,17	6,11,13,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,7,14	6,11,13,15	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,7,14,16,17,18	6,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,7,12	6,11	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,7,12,16,17,18	6,11,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,7,12,18	6,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,7,12,16,17	6,11,15,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,7,12,14,17,18	6,11,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,7,12,14,16	6,11	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,7,12,14,17	6,11,15,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,7,12,14,16,18	6,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,7,12,18	6,11,13,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,7,12,16,17	6,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,7,12	6,11,13,15	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,7,12,16,17,18	6,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,7,12,14,17	6,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,7,12,14,16,18	6,11,13,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,7,12,14,17,18	6,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,7,12,14,16	6,11,13,15	2^{-23}

Table 0.1331 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,7,10,18	6,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,7,10,16,17	6,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,7,10	6,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,7,10,16,17,18	6,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,7,10,14,17	6,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,7,10,14,16,18	6,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,7,10,14,17,18	6,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,7,10,14,16	6,15	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,7,10	6,13	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,7,10,16,17,18	6,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,7,10,18	6,13,15,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,7,10,16,17	6,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,7,10,14,17,18	6,13,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,7,10,14,16	6,13	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,7,10,14,17	6,13,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,7,10,14,16,18	6,13,15,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,7,10,12,17	6,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,7,10,12,16,18	6,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,7,10,12,17,18	6,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,7,10,12,16	6,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,7,10,12,14,18	6,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,7,10,12,14,16,17	6,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,7,10,12,14	6,15	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,7,10,12,14,16,17,18	6,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,7,10,12,17,18	6,13,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,7,10,12,16	6,13	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,7,10,12,17	6,13,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,7,10,12,16,18	6,13,15,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,7,10,12,14	6,13	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,7,10,12,14,16,17,18	6,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,7,10,12,14,18	6,13,15,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,7,10,12,14,16,17	6,13,15,17	$2^{-17.5}$

Table 0.1332 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,7,10	6,11	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,7,10,16,17,18	6,11,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,7,10,18	6,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,7,10,16,17	6,11,15,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,7,10,14,17,18	6,11,17,18	2^{-1}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,7,10,14,16	6,11	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,7,10,14,17	6,11,15,17	2^{-1}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,7,10,14,16,18	6,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,7,10,18	6,11,13,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,7,10,16,17	6,11,13,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,7,10	6,11,13,15	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,7,10,16,17,18	6,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,7,10,14,17	6,11,13,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,7,10,14,16,18	6,11,13,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,7,10,14,17,18	6,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,7,10,14,16	6,11,13,15	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,7,10,12,17,18	6,11,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,7,10,12,16	6,11	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,7,10,12,17	6,11,15,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,7,10,12,16,18	6,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,7,10,12,14	6,11	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,7,10,12,14,16,17,18	6,11,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,7,10,12,14,18	6,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,7,10,12,14,16,17	6,11,15,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,7,10,12,17	6,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,7,10,12,16,18	6,11,13,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,7,10,12,17,18	6,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,7,10,12,16	6,11,13,15	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,7,10,12,14,18	6,11,13,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,7,10,12,14,16,17	6,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,7,10,12,14	6,11,13,15	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,7,10,12,14,16,17,18	6,11,13,15,17,18	$2^{-17.5}$

Table 0.1333 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,7,17,18	6,9,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,7,16	6,9	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,7,17	6,9,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,7,16,18	6,9,15,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,7,14	6,9	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,7,14,16,17,18	6,9,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,7,14,18	6,9,15,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,7,14,16,17	6,9,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,7,17	6,9,13,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,7,16,18	6,9,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,7,17,18	6,9,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,7,16	6,9,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,7,14,18	6,9,13,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,7,14,16,17	6,9,13,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,7,14	6,9,13,15	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,7,14,16,17,18	6,9,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,7,12	6,9	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,7,12,16,17,18	6,9,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,7,12,18	6,9,15,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,7,12,16,17	6,9,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,7,12,14,17,18	6,9,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,7,12,14,16	6,9	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,7,12,14,17	6,9,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,7,12,14,16,18	6,9,15,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,7,12,18	6,9,13,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,7,12,16,17	6,9,13,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,7,12	6,9,13,15	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,7,12,16,17,18	6,9,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,12,14,17	6,9,13,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,7,12,14,16,18	6,9,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,12,14,17,18	6,9,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,7,12,14,16	6,9,13,15	$2^{-17.5}$

Table 0.1334 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,7,17	6,9,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,7,16,18	6,9,11,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,7,17,18	6,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,7,16	6,9,11,15	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,7,14,18	6,9,11,18	2^{-1}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,7,14,16,17	6,9,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,7,14	6,9,11,15	2^{-1}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,7,14,16,17,18	6,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,7,17,18	6,9,11,13,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,7,16	6,9,11,13	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,7,17	6,9,11,13,15,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,7,16,18	6,9,11,13,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,7,14	6,9,11,13	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,7,14,16,17,18	6,9,11,13,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,7,14,18	6,9,11,13,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,7,14,16,17	6,9,11,13,15,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,7,12,18	6,9,11,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,7,12,16,17	6,9,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,7,12	6,9,11,15	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,7,12,16,17,18	6,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,7,12,14,17	6,9,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,7,12,14,16,18	6,9,11,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,7,12,14,17,18	6,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,7,12,14,16	6,9,11,15	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,7,12	6,9,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,7,12,16,17,18	6,9,11,13,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,7,12,18	6,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,7,12,16,17	6,9,11,13,15,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,7,12,14,17,18	6,9,11,13,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,7,12,14,16	6,9,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,7,12,14,17	6,9,11,13,15,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,7,12,14,16,18	6,9,11,13,15,18	$2^{-17.5}$

Table 0.1335 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,7,10	6,9	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,7,10,16,17,18	6,9,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,7,10,18	6,9,15,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,7,10,16,17	6,9,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,7,10,14,17,18	6,9,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,7,10,14,16	6,9	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,7,10,14,17	6,9,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,7,10,14,16,18	6,9,15,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,7,10,18	6,9,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,7,10,16,17	6,9,13,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,7,10	6,9,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,7,10,16,17,18	6,9,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,7,10,14,17	6,9,13,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,7,10,14,16,18	6,9,13,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,7,10,14,17,18	6,9,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,7,10,14,16	6,9,13,15	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,7,10,12,17,18	6,9,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,7,10,12,16	6,9	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,7,10,12,17	6,9,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,7,10,12,16,18	6,9,15,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,7,10,12,14	6,9	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,7,10,12,14,16,17,18	6,9,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,7,10,12,14,18	6,9,15,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,7,10,12,14,16,17	6,9,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,7,10,12,17	6,9,13,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,7,10,12,16,18	6,9,13,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,7,10,12,17,18	6,9,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,7,10,12,16	6,9,13,15	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,7,10,12,14,18	6,9,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,7,10,12,14,16,17	6,9,13,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,7,10,12,14	6,9,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,7,10,12,14,16,17,18	6,9,13,15,17,18	2^{-23}

Table 0.1336 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,7,10,18	6,9,11,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,7,10,16,17	6,9,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,7,10	6,9,11,15	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,7,10,16,17,18	6,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,7,10,14,17	6,9,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,7,10,14,16,18	6,9,11,18	2^{-34}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,7,10,14,17,18	6,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,7,10,14,16	6,9,11,15	2^{-34}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,7,10	6,9,11,13	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,7,10,16,17,18	6,9,11,13,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,7,10,18	6,9,11,13,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,7,10,16,17	6,9,11,13,15,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,7,10,14,17,18	6,9,11,13,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,7,10,14,16	6,9,11,13	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,7,10,14,17	6,9,11,13,15,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,7,10,14,16,18	6,9,11,13,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,7,10,12,17	6,9,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,7,10,12,16,18	6,9,11,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,7,10,12,17,18	6,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,7,10,12,16	6,9,11,15	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,7,10,12,14,18	6,9,11,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,7,10,12,14,16,17	6,9,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,7,10,12,14	6,9,11,15	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,7,10,12,14,16,17,18	6,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,7,10,12,17,18	6,9,11,13,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,7,10,12,16	6,9,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,7,10,12,17	6,9,11,13,15,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,7,10,12,16,18	6,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,7,10,12,14	6,9,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,7,10,12,14,16,17,18	6,9,11,13,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,7,10,12,14,18	6,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,7,10,12,14,16,17	6,9,11,13,15,17	2^{-23}

Table 0.1337 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,7,18	6,8,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,7,16,17	6,8,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,7	6,8,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,7,16,17,18	6,8,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,7,14,17	6,8,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,7,14,16,18	6,8,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,7,14,17,18	6,8,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,7,14,16	6,8,15	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,7	6,8,13	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,7,16,17,18	6,8,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,7,18	6,8,13,15,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,7,16,17	6,8,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,7,14,17,18	6,8,13,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,7,14,16	6,8,13	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,7,14,17	6,8,13,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,7,14,16,18	6,8,13,15,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,7,12,17	6,8,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,7,12,16,18	6,8,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,7,12,17,18	6,8,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,7,12,16	6,8,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,7,12,14,18	6,8,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,7,12,14,16,17	6,8,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,7,12,14	6,8,15	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,7,12,14,16,17,18	6,8,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,7,12,17,18	6,8,13,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,7,12,16	6,8,13	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,7,12,17	6,8,13,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,7,12,16,18	6,8,13,15,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,7,12,14	6,8,13	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,7,12,14,16,17,18	6,8,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,7,12,14,18	6,8,13,15,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,7,12,14,16,17	6,8,13,15,17	$2^{-17.5}$

Table 0.1338 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,7	6,8,11	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,7,16,17,18	6,8,11,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,7,18	6,8,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,7,16,17	6,8,11,15,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,7,14,17,18	6,8,11,17,18	2^{-34}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,7,14,16	6,8,11	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,7,14,17	6,8,11,15,17	2^{-34}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,7,14,16,18	6,8,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,7,18	6,8,11,13,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,7,16,17	6,8,11,13,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,7	6,8,11,13,15	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,7,16,17,18	6,8,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,7,14,17	6,8,11,13,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,7,14,16,18	6,8,11,13,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,7,14,17,18	6,8,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,7,14,16	6,8,11,13,15	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,7,12,17,18	6,8,11,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,7,12,16	6,8,11	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,7,12,17	6,8,11,15,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,7,12,16,18	6,8,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,7,12,14	6,8,11	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,7,12,14,16,17,18	6,8,11,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,7,12,14,18	6,8,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,7,12,14,16,17	6,8,11,15,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,7,12,17	6,8,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,7,12,16,18	6,8,11,13,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,7,12,17,18	6,8,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,7,12,16	6,8,11,13,15	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,7,12,14,18	6,8,11,13,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,7,12,14,16,17	6,8,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,7,12,14	6,8,11,13,15	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,7,12,14,16,17,18	6,8,11,13,15,17,18	$2^{-17.5}$

Table 0.1339 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,7,10,17	6,8,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,7,10,16,18	6,8,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,7,10,17,18	6,8,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,7,10,16	6,8,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,7,10,14,18	6,8,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,7,10,14,16,17	6,8,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,7,10,14	6,8,15	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,7,10,14,16,17,18	6,8,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,7,10,17,18	6,8,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,7,10,16	6,8,13	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,7,10,17	6,8,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,7,10,16,18	6,8,13,15,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,7,10,14	6,8,13	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,7,10,14,16,17,18	6,8,13,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,7,10,14,18	6,8,13,15,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,7,10,14,16,17	6,8,13,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,7,10,12,18	6,8,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,7,10,12,16,17	6,8,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,7,10,12	6,8,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,7,10,12,16,17,18	6,8,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,7,10,12,14,17	6,8,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,7,10,12,14,16,18	6,8,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,7,10,12,14,17,18	6,8,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,7,10,12,14,16	6,8,15	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,7,10,12	6,8,13	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,7,10,12,16,17,18	6,8,13,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,7,10,12,18	6,8,13,15,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,7,10,12,16,17	6,8,13,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,7,10,12,14,17,18	6,8,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,10,12,14,16	6,8,13	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,7,10,12,14,17	6,8,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,10,12,14,16,18	6,8,13,15,18	2^{-12}

Table 0.1340 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,7,10,17,18	6,8,11,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,7,10,16	6,8,11	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,7,10,17	6,8,11,15,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,7,10,16,18	6,8,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,7,10,14	6,8,11	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,7,10,14,16,17,18	6,8,11,17,18	2^{-1}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,7,10,14,18	6,8,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,7,10,14,16,17	6,8,11,15,17	2^{-1}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,7,10,17	6,8,11,13,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,7,10,16,18	6,8,11,13,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,7,10,17,18	6,8,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,7,10,16	6,8,11,13,15	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,7,10,14,18	6,8,11,13,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,7,10,14,16,17	6,8,11,13,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,7,10,14	6,8,11,13,15	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,7,10,14,16,17,18	6,8,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,7,10,12	6,8,11	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,7,10,12,16,17,18	6,8,11,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,7,10,12,18	6,8,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,7,10,12,16,17	6,8,11,15,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,7,10,12,14,17,18	6,8,11,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,7,10,12,14,16	6,8,11	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,7,10,12,14,17	6,8,11,15,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,7,10,12,14,16,18	6,8,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,7,10,12,18	6,8,11,13,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,7,10,12,16,17	6,8,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,7,10,12	6,8,11,13,15	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,7,10,12,16,17,18	6,8,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,7,10,12,14,17	6,8,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,7,10,12,14,16,18	6,8,11,13,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,7,10,12,14,17,18	6,8,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,7,10,12,14,16	6,8,11,13,15	2^{-12}

Table 0.1341 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,7	6,8,9	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,7,16,17,18	6,8,9,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,7,18	6,8,9,15,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,7,16,17	6,8,9,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,7,14,17,18	6,8,9,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,7,14,16	6,8,9	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,7,14,17	6,8,9,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,7,14,16,18	6,8,9,15,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,7,18	6,8,9,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,7,16,17	6,8,9,13,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,7	6,8,9,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,7,16,17,18	6,8,9,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,7,14,17	6,8,9,13,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,7,14,16,18	6,8,9,13,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,7,14,17,18	6,8,9,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,7,14,16	6,8,9,13,15	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,7,12,17,18	6,8,9,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,7,12,16	6,8,9	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,7,12,17	6,8,9,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,7,12,16,18	6,8,9,15,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,7,12,14	6,8,9	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,7,12,14,16,17,18	6,8,9,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,7,12,14,18	6,8,9,15,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,7,12,14,16,17	6,8,9,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,7,12,17	6,8,9,13,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,7,12,16,18	6,8,9,13,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,7,12,17,18	6,8,9,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,7,12,16	6,8,9,13,15	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,7,12,14,18	6,8,9,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,7,12,14,16,17	6,8,9,13,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,7,12,14	6,8,9,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,7,12,14,16,17,18	6,8,9,13,15,17,18	2^{-12}

Table 0.1342 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,7,18	6,8,9,11,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,7,16,17	6,8,9,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,7	6,8,9,11,15	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,7,16,17,18	6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,7,14,17	6,8,9,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,7,14,16,18	6,8,9,11,18	2^{-1}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,7,14,17,18	6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,7,14,16	6,8,9,11,15	2^{-1}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,7	6,8,9,11,13	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,7,16,17,18	6,8,9,11,13,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,7,18	6,8,9,11,13,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,7,16,17	6,8,9,11,13,15,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,7,14,17,18	6,8,9,11,13,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,7,14,16	6,8,9,11,13	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,7,14,17	6,8,9,11,13,15,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,7,14,16,18	6,8,9,11,13,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,7,12,17	6,8,9,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,7,12,16,18	6,8,9,11,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,7,12,17,18	6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,7,12,16	6,8,9,11,15	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,7,12,14,18	6,8,9,11,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,7,12,14,16,17	6,8,9,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,7,12,14	6,8,9,11,15	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,7,12,14,16,17,18	6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,7,12,17,18	6,8,9,11,13,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,7,12,16	6,8,9,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,7,12,17	6,8,9,11,13,15,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,7,12,16,18	6,8,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,7,12,14	6,8,9,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,7,12,14,16,17,18	6,8,9,11,13,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,7,12,14,18	6,8,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,7,12,14,16,17	6,8,9,11,13,15,17	2^{-12}

Table 0.1343 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,7,10,17,18	6,8,9,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,7,10,16	6,8,9	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,7,10,17	6,8,9,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,7,10,16,18	6,8,9,15,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,7,10,14	6,8,9	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,7,10,14,16,17,18	6,8,9,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,7,10,14,18	6,8,9,15,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,7,10,14,16,17	6,8,9,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,7,10,17	6,8,9,13,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,7,10,16,18	6,8,9,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,7,10,17,18	6,8,9,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,7,10,16	6,8,9,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,7,10,14,18	6,8,9,13,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,7,10,14,16,17	6,8,9,13,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,7,10,14	6,8,9,13,15	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,7,10,14,16,17,18	6,8,9,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,7,10,12	6,8,9	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,7,10,12,16,17,18	6,8,9,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,7,10,12,18	6,8,9,15,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,7,10,12,16,17	6,8,9,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,7,10,12,14,17,18	6,8,9,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,7,10,12,14,16	6,8,9	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,7,10,12,14,17	6,8,9,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,7,10,12,14,16,18	6,8,9,15,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,7,10,12,18	6,8,9,13,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,7,10,12,16,17	6,8,9,13,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,7,10,12	6,8,9,13,15	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,7,10,12,16,17,18	6,8,9,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,7,10,12,14,17	6,8,9,13,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,7,10,12,14,16,18	6,8,9,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,7,10,12,14,17,18	6,8,9,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,7,10,12,14,16	6,8,9,13,15	$2^{-17.5}$

Table 0.1344 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,7,10,17	6,8,9,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,7,10,16,18	6,8,9,11,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,7,10,17,18	6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,7,10,16	6,8,9,11,15	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,7,10,14,18	6,8,9,11,18	2^{-34}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,7,10,14,16,17	6,8,9,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,7,10,14	6,8,9,11,15	2^{-34}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,7,10,14,16,17,18	6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,7,10,17,18	6,8,9,11,13,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,7,10,16	6,8,9,11,13	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,7,10,17	6,8,9,11,13,15,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,7,10,16,18	6,8,9,11,13,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,7,10,14	6,8,9,11,13	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,7,10,14,16,17,18	6,8,9,11,13,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,7,10,14,18	6,8,9,11,13,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,7,10,14,16,17	6,8,9,11,13,15,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,7,10,12,18	6,8,9,11,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,7,10,12,16,17	6,8,9,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,7,10,12	6,8,9,11,15	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,7,10,12,16,17,18	6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,7,10,12,14,17	6,8,9,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,7,10,12,14,16,18	6,8,9,11,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,7,10,12,14,17,18	6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,7,10,12,14,16	6,8,9,11,15	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,7,10,12	6,8,9,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,7,10,12,16,17,18	6,8,9,11,13,17,18	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,7,10,12,18	6,8,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,7,10,12,16,17	6,8,9,11,13,15,17	2^{-12}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,7,10,12,14,17,18	6,8,9,11,13,17,18	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,7,10,12,14,16	6,8,9,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,7,10,12,14,17	6,8,9,11,13,15,17	2^{-23}
$(1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,7,10,12,14,16,18	6,8,9,11,13,15,18	$2^{-17.5}$

Table 0.1345 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,18	18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,16,17	17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,5	15	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,16,17,18	15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,14,17	17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,14,16,18	18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,14,17,18	15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,14,16	15	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,5	13	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,16,17,18	13,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,18	13,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,16,17	13,15,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,14,17,18	13,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,14,16	13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,14,17	13,15,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,14,16,18	13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,12,17	17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,12,16,18	18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,12,17,18	15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,12,16	15	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,12,14,18	18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,12,17,18	15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,12,14	15	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,12,14,16,17,18	15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,12,17,18	13,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,12,16	13	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,12,17	13,15,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,12,16,18	13,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,12,14	13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,12,14,16,17,18	13,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,12,14,18	13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,12,14,16,17	13,15,17	2^{-23}

Table 0.1346 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,5	11	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,16,17,18	11,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,18	11,15,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,16,17	11,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,14,17,18	11,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,14,16	11	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,14,17	11,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,14,16,18	11,15,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,18	11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,16,17	11,13,17	2^{-34}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,5	11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,16,17,18	11,13,15,17,18	2^{-34}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,14,17	11,13,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,14,16,18	11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,14,17,18	11,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,14,16	11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,12,17,18	11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,12,16	11	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,12,17	11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,12,16,18	11,15,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,12,14	11	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,12,14,16,17,18	11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,12,14,18	11,15,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,12,14,16,17	11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,12,17	11,13,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,12,16,18	11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,12,17,18	11,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,12,16	11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,12,14,18	11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,12,14,16,17	11,13,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,12,14	11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,12,14,16,17,18	11,13,15,17,18	2^{-23}

Table 0.1347 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,10,17	17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,10,16,18	18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,10,17,18	15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,10,16	15	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,10,14,18	18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,10,14,16,17	17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,10,14	15	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,10,14,16,17,18	15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,10,17,18	13,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,10,16	13	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,10,17	13,15,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,10,16,18	13,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,10,14	13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,10,14,16,17,18	13,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,10,14,18	13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,10,14,16,17	13,15,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,10,12,18	18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,10,12,16,17	17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,10,12	15	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,10,12,16,17,18	15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,10,12,14,17	17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,10,12,14,16,18	18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,10,12,14,17,18	15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,10,12,14,16	15	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,10,12	13	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,10,12,16,17,18	13,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,10,12,18	13,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,10,12,16,17	13,15,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,10,12,14,17,18	13,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,10,12,14,16	13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,10,12,14,17	13,15,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,10,12,14,16,18	13,15,18	$2^{-17.5}$

Table 0.1348 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,10,17,18	11,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,10,16	11	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,10,17	11,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,10,16,18	11,15,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,10,14	11	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,10,14,16,17,18	11,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,10,14,18	11,15,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,10,14,16,17	11,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,10,17	11,13,17	2^{-1}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,10,16,18	11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,10,17,18	11,13,15,17,18	2^{-1}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,10,16	11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,10,14,18	11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,10,14,16,17	11,13,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,10,14	11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,10,14,16,17,18	11,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,10,12	11	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,10,12,16,17,18	11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,10,12,18	11,15,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,10,12,16,17	11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,10,12,14,17,18	11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,10,12,14,16	11	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,10,12,14,17	11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,10,12,14,16,18	11,15,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,10,12,18	11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,10,12,16,17	11,13,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,10,12	11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,10,12,16,17,18	11,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,10,12,14,17	11,13,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,10,12,14,16,18	11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,10,12,14,17,18	11,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,10,12,14,16	11,13,15	$2^{-17.5}$

Table 0.1349 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,5	9	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,16,17,18	9,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,18	9,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,16,17	9,15,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,14,17,18	9,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,14,16	9	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,14,17	9,15,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,14,16,18	9,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,18	9,13,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,16,17	9,13,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,5	9,13,15	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,16,17,18	9,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,14,17	9,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,14,16,18	9,13,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,14,17,18	9,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,14,16	9,13,15	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,12,17,18	9,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,12,16	9	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,12,17	9,15,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,12,16,18	9,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,12,14	9	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,12,14,16,17,18	9,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,12,14,18	9,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,12,14,16,17	9,15,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,12,17	9,13,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,12,16,18	9,13,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,12,17,18	9,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,12,16	9,13,15	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,12,14,18	9,13,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,12,14,16,17	9,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,12,14	9,13,15	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,12,14,16,17,18	9,13,15,17,18	$2^{-17.5}$

Table 0.1350 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,18	9,11,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,16,17	9,11,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,5	9,11,15	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,16,17,18	9,11,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,14,17	9,11,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,14,16,18	9,11,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,14,17,18	9,11,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,14,16	9,11,15	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,5	9,11,13	2^{-1}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,16,17,18	9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,18	9,11,13,15,18	2^{-1}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,16,17	9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,14,17,18	9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,14,16	9,11,13	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,14,17	9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,14,16,18	9,11,13,15,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,12,17	9,11,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,12,16,18	9,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,12,17,18	9,11,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,12,16	9,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,12,14,18	9,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,12,14,16,17	9,11,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,12,14	9,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,12,14,16,17,18	9,11,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,12,17,18	9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,12,16	9,11,13	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,12,17	9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,12,16,18	9,11,13,15,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,12,14	9,11,13	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,12,14,16,17,18	9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,12,14,18	9,11,13,15,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,12,14,16,17	9,11,13,15,17	$2^{-17.5}$

Table 0.1351 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,10,17,18	9,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,10,16	9	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,10,17	9,15,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,10,16,18	9,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,10,14	9	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,10,14,16,17,18	9,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,10,14,18	9,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,10,14,16,17	9,15,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,10,17	9,13,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,10,16,18	9,13,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,10,17,18	9,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,10,16	9,13,15	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,10,14,18	9,13,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,10,14,16,17	9,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,10,14	9,13,15	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,10,14,16,17,18	9,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,10,12	9	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,10,12,16,17,18	9,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,10,12,18	9,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,10,12,16,17	9,15,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,10,12,14,17,18	9,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,10,12,14,16	9	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,10,12,14,17	9,15,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,10,12,14,16,18	9,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,10,12,18	9,13,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,10,12,16,17	9,13,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,10,12	9,13,15	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,10,12,16,17,18	9,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,10,12,14,17	9,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,10,12,14,16,18	9,13,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,10,12,14,17,18	9,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,10,12,14,16	9,13,15	2^{-23}

Table 0.1352 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,10,17	9,11,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,10,16,18	9,11,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,10,17,18	9,11,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,10,16	9,11,15	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,10,14,18	9,11,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,10,14,16,17	9,11,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,10,14	9,11,15	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,10,14,16,17,18	9,11,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,10,17,18	9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,10,16	9,11,13	2^{-34}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,10,17	9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,10,16,18	9,11,13,15,18	2^{-34}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,10,14	9,11,13	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,10,14,16,17,18	9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,10,14,18	9,11,13,15,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,10,14,16,17	9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,10,12,18	9,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,10,12,16,17	9,11,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,10,12	9,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,10,12,16,17,18	9,11,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,10,12,14,17	9,11,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,10,12,14,16,18	9,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,10,12,14,17,18	9,11,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,10,12,14,16	9,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,10,12	9,11,13	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,10,12,16,17,18	9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,10,12,18	9,11,13,15,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,10,12,16,17	9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,10,12,14,17,18	9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,10,12,14,16	9,11,13	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,10,12,14,17	9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,10,12,14,16,18	9,11,13,15,18	2^{-23}

Table 0.1353 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,17	8,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,16,18	8,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,17,18	8,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,16	8,15	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,14,18	8,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,14,16,17	8,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,14	8,15	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,14,16,17,18	8,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,17,18	8,13,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,16	8,13	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,17	8,13,15,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,16,18	8,13,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,14	8,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,14,16,17,18	8,13,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,14,18	8,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,14,16,17	8,13,15,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,12,18	8,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,12,16,17	8,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,12	8,15	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,12,16,17,18	8,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,12,14,17	8,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,12,14,16,18	8,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,12,14,17,18	8,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,12,14,16	8,15	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,12	8,13	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,12,16,17,18	8,13,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,12,18	8,13,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,12,16,17	8,13,15,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,12,14,17,18	8,13,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,12,14,16	8,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,12,14,17	8,13,15,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,12,14,16,18	8,13,15,18	$2^{-17.5}$

Table 0.1354 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,17,18	8,11,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,16	8,11	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,17	8,11,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,16,18	8,11,15,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,14	8,11	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,14,16,17,18	8,11,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,14,18	8,11,15,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,14,16,17	8,11,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,17	8,11,13,17	2^{-34}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,16,18	8,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,17,18	8,11,13,15,17,18	2^{-34}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,16	8,11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,14,18	8,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,14,16,17	8,11,13,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,14	8,11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,14,16,17,18	8,11,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,12	8,11	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,12,16,17,18	8,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,12,18	8,11,15,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,12,16,17	8,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,12,14,17,18	8,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,12,14,16	8,11	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,12,14,17	8,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,12,14,16,18	8,11,15,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,12,18	8,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,12,16,17	8,11,13,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,12	8,11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,12,16,17,18	8,11,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,12,14,17	8,11,13,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,12,14,16,18	8,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,12,14,17,18	8,11,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,12,14,16	8,11,13,15	$2^{-17.5}$

Table 0.1355 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,10,18	8,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,10,16,17	8,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,10	8,15	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,10,16,17,18	8,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,10,14,17	8,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,10,14,16,18	8,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,10,14,17,18	8,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,10,14,16	8,15	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,10	8,13	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,10,16,17,18	8,13,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,10,18	8,13,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,10,16,17	8,13,15,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,10,14,17,18	8,13,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,10,14,16	8,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,10,14,17	8,13,15,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,10,14,16,18	8,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,10,12,17	8,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,10,12,16,18	8,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,10,12,17,18	8,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,10,12,16	8,15	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,10,12,14,18	8,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,10,12,17,18	8,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,10,12,14,16,17	8,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,10,12,14	8,15	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,10,12,14,16,17,18	8,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,10,12,17,18	8,13,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,10,12,16	8,13	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,10,12,17	8,13,15,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,10,12,16,18	8,13,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,10,12,14	8,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,10,12,14,16,17,18	8,13,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,10,12,14,18	8,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,10,12,14,16,17	8,13,15,17	2^{-12}

Table 0.1356 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,10	8,11	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,10,16,17,18	8,11,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,10,18	8,11,15,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,10,16,17	8,11,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,10,14,17,18	8,11,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,10,14,16	8,11	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,10,14,17	8,11,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,10,14,16,18	8,11,15,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,10,18	8,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,10,16,17	8,11,13,17	2^{-1}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,10	8,11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,10,16,17,18	8,11,13,15,17,18	2^{-1}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,10,14,17	8,11,13,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,10,14,16,18	8,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,10,14,17,18	8,11,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,10,14,16	8,11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,10,12,17,18	8,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,10,12,16	8,11	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,10,12,17	8,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,10,12,16,18	8,11,15,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,10,12,14	8,11	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,10,12,14,16,17,18	8,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,10,12,14,18	8,11,15,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,10,12,14,16,17	8,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,10,12,17	8,11,13,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,10,12,16,18	8,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,10,12,17,18	8,11,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,10,12,16	8,11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,10,12,14,18	8,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,10,12,14,16,17	8,11,13,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,10,12,14	8,11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,10,12,14,16,17,18	8,11,13,15,17,18	2^{-12}

Table 0.1357 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,17,18	8,9,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,16	8,9	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,17	8,9,15,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,16,18	8,9,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,14	8,9	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,14,16,17,18	8,9,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,14,18	8,9,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,14,16,17	8,9,15,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,17	8,9,13,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,16,18	8,9,13,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,17,18	8,9,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,16	8,9,13,15	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,14,18	8,9,13,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,14,16,17	8,9,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,14	8,9,13,15	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,14,16,17,18	8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,12	8,9	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,12,16,17,18	8,9,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,12,18	8,9,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,12,16,17	8,9,15,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,12,14,17,18	8,9,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,12,14,16	8,9	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,12,14,17	8,9,15,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,12,14,16,18	8,9,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,12,18	8,9,13,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,12,16,17	8,9,13,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,12	8,9,13,15	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,12,16,17,18	8,9,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,12,14,17	8,9,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,12,14,16,18	8,9,13,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,12,14,17,18	8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,12,14,16	8,9,13,15	2^{-12}

Table 0.1358 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,17	8,9,11,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,16,18	8,9,11,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,17,18	8,9,11,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,16	8,9,11,15	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,14,18	8,9,11,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,14,16,17	8,9,11,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,14	8,9,11,15	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,14,16,17,18	8,9,11,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,17,18	8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,16	8,9,11,13	2^{-1}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,17	8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,16,18	8,9,11,13,15,18	2^{-1}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,14	8,9,11,13	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,14,16,17,18	8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,14,18	8,9,11,13,15,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,14,16,17	8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,12,18	8,9,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,12,16,17	8,9,11,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,12	8,9,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,12,16,17,18	8,9,11,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,12,14,17	8,9,11,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,12,14,16,18	8,9,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,12,14,17,18	8,9,11,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,12,14,16	8,9,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,12	8,9,11,13	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,12,16,17,18	8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,12,18	8,9,11,13,15,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,12,16,17	8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,12,14,17,18	8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,12,14,16	8,9,11,13	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,12,14,17	8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,12,14,16,18	8,9,11,13,15,18	2^{-12}

Table 0.1359 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,10	8,9	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,10,16,17,18	8,9,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,10,18	8,9,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,10,16,17	8,9,15,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,10,14,17,18	8,9,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,10,14,16	8,9	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,10,14,17	8,9,15,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,10,14,16,18	8,9,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,10,18	8,9,13,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,10,16,17	8,9,13,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,10	8,9,13,15	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,10,16,17,18	8,9,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,10,14,17	8,9,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,10,14,16,18	8,9,13,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,10,14,17,18	8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,10,14,16	8,9,13,15	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,10,12,17,18	8,9,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,10,12,16	8,9	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,10,12,17	8,9,15,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,10,12,16,18	8,9,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,10,12,14	8,9	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,10,12,14,16,17,18	8,9,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,10,12,14,18	8,9,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,10,12,14,16,17	8,9,15,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,10,12,17	8,9,13,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,10,12,16,18	8,9,13,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,10,12,17,18	8,9,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,10,12,16	8,9,13,15	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,10,12,14,18	8,9,13,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,10,12,14,16,17	8,9,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,10,12,14	8,9,13,15	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,10,12,14,16,17,18	8,9,13,15,17,18	$2^{-17.5}$

Table 0.1360 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,10,18	8,9,11,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,10,16,17	8,9,11,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,10	8,9,11,15	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,10,16,17,18	8,9,11,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,10,14,17	8,9,11,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,10,14,16,18	8,9,11,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,10,14,17,18	8,9,11,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,10,14,16	8,9,11,15	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,10	8,9,11,13	2^{-34}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,10,16,17,18	8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,10,18	8,9,11,13,15,18	2^{-34}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,10,16,17	8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,10,14,17,18	8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,10,14,16	8,9,11,13	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,10,14,17	8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,10,14,16,18	8,9,11,13,15,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,10,12,17	8,9,11,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,10,12,16,18	8,9,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,10,12,17,18	8,9,11,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,10,12,16	8,9,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,10,12,14,18	8,9,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,10,12,14,16,17	8,9,11,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,10,12,14	8,9,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,10,12,14,16,17,18	8,9,11,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,10,12,17,18	8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,10,12,16	8,9,11,13	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,10,12,17	8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,10,12,16,18	8,9,11,13,15,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,10,12,14	8,9,11,13	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,10,12,14,16,17,18	8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,10,12,14,18	8,9,11,13,15,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,10,12,14,16,17	8,9,11,13,15,17	$2^{-17.5}$

Table 0.1361 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,7	—	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,7,16,17,18	17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,7,18	15,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,7,16,17	15,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,7,14,17,18	17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,7,14,16	—	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,7,14,17	15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,7,14,16,18	15,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,7,18	13,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,7,16,17	13,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7	13,15	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,7,16,17,18	13,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,7,14,17	13,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,7,14,16,18	13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,7,14,17,18	13,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,7,14,16	13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,7,12,17,18	17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,7,12,16	—	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,7,12,17	15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,7,12,16,18	15,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,7,12,14	—	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,7,12,14,16,17,18	17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,7,12,14,18	15,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,7,12,14,16,17	15,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,7,12,17	13,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,7,12,16,18	13,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,7,12,17,18	13,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,7,12,16	13,15	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,7,12,14,18	13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,7,12,14,16,17	13,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,7,12,14	13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,12,14,16,17,18	13,15,17,18	2^{-23}

Table 0.1362 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,7,18	11,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7,16,17	11,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,7	11,15	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,7,16,17,18	11,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,7,14,17	11,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,7,14,16,18	11,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,7,14,17,18	11,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,7,14,16	11,15	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,7	11,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,7,16,17,18	11,13,17,18	2^{-34}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,7,18	11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,7,16,17	11,13,15,17	2^{-34}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,7,14,17,18	11,13,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,7,14,16	11,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,7,14,17	11,13,15,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,7,14,16,18	11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,7,12,17	11,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,7,12,16,18	11,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,7,12,17,18	11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,7,12,16	11,15	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,7,12,14,18	11,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,7,12,14,16,17	11,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,7,12,14	11,15	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,7,12,14,16,17,18	11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,7,12,17,18	11,13,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,7,12,16	11,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,7,12,17	11,13,15,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,7,12,16,18	11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,7,12,14	11,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,7,12,14,16,17,18	11,13,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,7,12,14,18	11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,7,12,14,16,17	11,13,15,17	2^{-23}

Table 0.1363 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,10,17,18	17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,7,10,16	—	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,7,10,17	15,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,7,10,16,18	15,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,7,10,14	—	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,7,10,14,16,17,18	17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,7,10,14,18	15,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,7,10,14,16,17	15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,7,10,17	13,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,7,10,16,18	13,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,7,10,17,18	13,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,7,10,16	13,15	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,7,10,14,18	13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,7,10,14,16,17	13,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,7,10,14	13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,7,10,14,16,17,18	13,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,12	—	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,10,12,16,17,18	17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,12,18	15,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,10,12,16,17	15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,7,10,12,14,17,18	17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,7,10,12,14,16	—	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,10,12,14,17	15,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,7,10,12,14,16,18	15,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,7,10,12,18	13,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,10,12,16,17	13,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,12	13,15	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,10,12,16,17,18	13,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,10,12,14,17	13,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,7,10,12,14,16,18	13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,10,12,14,17,18	13,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,7,10,12,14,16	13,15	$2^{-17.5}$

Table 0.1364 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,7,10,17	11,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,7,10,16,18	11,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,7,10,17,18	11,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,7,10,16	11,15	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,7,10,14,18	11,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,7,10,14,16,17	11,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,7,10,14	11,15	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,7,10,14,16,17,18	11,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,7,10,17,18	11,13,17,18	2^{-1}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,7,10,16	11,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,7,10,17	11,13,15,17	2^{-1}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,7,10,16,18	11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,10,14	11,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,7,10,14,16,17,18	11,13,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,10,14,18	11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,7,10,14,16,17	11,13,15,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,7,10,12,18	11,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,7,10,12,16,17	11,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,7,10,12	11,15	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,7,10,12,16,17,18	11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,7,10,12,14,17	11,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,7,10,12,14,16,18	11,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,7,10,12,14,17,18	11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,7,10,12,14,16	11,15	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,7,10,12	11,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,7,10,12,16,17,18	11,13,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,7,10,12,18	11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,7,10,12,16,17	11,13,15,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,7,10,12,14,17,18	11,13,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,7,10,12,14,16	11,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,7,10,12,14,17	11,13,15,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,7,10,12,14,16,18	11,13,15,18	$2^{-17.5}$

Table 0.1365 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,7,18	9,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,7,16,17	9,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,7	9,15	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,7,16,17,18	9,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,7,14,17	9,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,7,14,16,18	9,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,7,14,17,18	9,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,7,14,16	9,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,7	9,13	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,7,16,17,18	9,13,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,7,18	9,13,15,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,7,16,17	9,13,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,7,14,17,18	9,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,7,14,16	9,13	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,7,14,17	9,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,7,14,16,18	9,13,15,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,7,12,17	9,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,7,12,16,18	9,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,7,12,17,18	9,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,7,12,16	9,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,7,12,14,18	9,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,7,12,14,16,17	9,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,7,12,14	9,15	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,7,12,14,16,17,18	9,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,7,12,17,18	9,13,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,7,12,16	9,13	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,7,12,17	9,13,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,7,12,16,18	9,13,15,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,7,12,14	9,13	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,7,12,14,16,17,18	9,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,7,12,14,18	9,13,15,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,7,12,14,16,17	9,13,15,17	$2^{-17.5}$

Table 0.1366 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,7	9,11	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,7,16,17,18	9,11,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,7,18	9,11,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,7,16,17	9,11,15,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,7,14,17,18	9,11,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,7,14,16	9,11	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,7,14,17	9,11,15,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,7,14,16,18	9,11,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,7,18	9,11,13,18	2^{-1}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,7,16,17	9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,7	9,11,13,15	2^{-1}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,7,16,17,18	9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,7,14,17	9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,7,14,16,18	9,11,13,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,7,14,17,18	9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,7,14,16	9,11,13,15	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,7,12,17,18	9,11,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,7,12,16	9,11	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,7,12,17	9,11,15,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,7,12,16,18	9,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,7,12,14	9,11	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7,12,14,16,17,18	9,11,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,7,12,14,18	9,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7,12,14,16,17	9,11,15,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,7,12,17	9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,7,12,16,18	9,11,13,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,7,12,17,18	9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,7,12,16	9,11,13,15	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,7,12,14,18	9,11,13,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,7,12,14,16,17	9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,7,12,14	9,11,13,15	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,7,12,14,16,17,18	9,11,13,15,17,18	$2^{-17.5}$

Table 0.1367 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,7,10,17	9,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,7,10,16,18	9,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,7,10,17,18	9,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,7,10,16	9,15	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,7,10,14,18	9,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,7,10,14,16,17	9,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,7,10,14	9,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,7,10,14,16,17,18	9,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,7,10,17,18	9,13,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,7,10,16	9,13	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,7,10,17	9,13,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,7,10,16,18	9,13,15,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,7,10,14	9,13	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,7,10,14,16,17,18	9,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,7,10,14,18	9,13,15,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,7,10,14,16,17	9,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,7,10,12,18	9,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,7,10,12,16,17	9,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,7,10,12	9,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,7,10,12,16,17,18	9,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,7,10,12,14,17	9,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,7,10,12,14,16,18	9,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,7,10,12,14,17,18	9,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,7,10,12,14,16	9,15	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,7,10,12	9,13	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,7,10,12,16,17,18	9,13,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,7,10,12,18	9,13,15,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,7,10,12,16,17	9,13,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,7,10,12,14,17,18	9,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,7,10,12,14,16	9,13	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,7,10,12,14,17	9,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,7,10,12,14,16,18	9,13,15,18	2^{-23}

Table 0.1368 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,7,10,17,18	9,11,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,7,10,16	9,11	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,7,10,17	9,11,15,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,7,10,16,18	9,11,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,7,10,14	9,11	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,7,10,14,16,17,18	9,11,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,7,10,14,18	9,11,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,7,10,14,16,17	9,11,15,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,7,10,17	9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,7,10,16,18	9,11,13,18	2^{-34}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,7,10,17,18	9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,7,10,16	9,11,13,15	2^{-34}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,7,10,14,18	9,11,13,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,7,10,14,16,17	9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,7,10,14	9,11,13,15	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,7,10,14,16,17,18	9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,7,10,12	9,11	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,7,10,12,16,17,18	9,11,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,7,10,12,18	9,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,7,10,12,16,17	9,11,15,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,7,10,12,14,17,18	9,11,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,7,10,12,14,16	9,11	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,7,10,12,14,17	9,11,15,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,7,10,12,14,16,18	9,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,7,10,12,18	9,11,13,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,7,10,12,16,17	9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,7,10,12	9,11,13,15	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,7,10,12,16,17,18	9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,7,10,12,14,17	9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,7,10,12,14,16,18	9,11,13,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,7,10,12,14,17,18	9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,7,10,12,14,16	9,11,13,15	2^{-23}

Table 0.1369 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,7,17,18	8,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,7,16	8	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,7,17	8,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,7,16,18	8,15,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,7,14	8	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,7,14,16,17,18	8,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,7,14,18	8,15,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,7,14,16,17	8,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,7,17	8,13,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,7,16,18	8,13,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,7,17,18	8,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,7,16	8,13,15	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,7,14,18	8,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,7,14,16,17	8,13,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,7,14	8,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,7,14,16,17,18	8,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,7,12	8	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,7,12,16,17,18	8,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,7,12,18	8,15,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,7,12,16,17	8,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,7,12,14,17,18	8,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,7,12,14,16	8	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,7,12,14,17	8,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,7,12,14,16,18	8,15,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,7,12,18	8,13,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,7,12,16,17	8,13,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,7,12	8,13,15	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,7,12,16,17,18	8,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,7,12,14,17	8,13,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,7,12,14,16,18	8,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,12,14,17,18	8,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,7,12,14,16	8,13,15	$2^{-17.5}$

Table 0.1370 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,7,17	8,11,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,7,16,18	8,11,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,7,17,18	8,11,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,7,16	8,11,15	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,7,14,18	8,11,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,7,14,16,17	8,11,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,7,14	8,11,15	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,7,14,16,17,18	8,11,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,7,17,18	8,11,13,17,18	2^{-34}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,7,16	8,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,7,17	8,11,13,15,17	2^{-34}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,7,16,18	8,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,7,14	8,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,7,14,16,17,18	8,11,13,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,7,14,18	8,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,7,14,16,17	8,11,13,15,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,7,12,18	8,11,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,7,12,16,17	8,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,7,12	8,11,15	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,7,12,16,17,18	8,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,7,12,14,17	8,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,7,12,14,16,18	8,11,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,7,12,14,17,18	8,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,7,12,14,16	8,11,15	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,7,12	8,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,7,12,16,17,18	8,11,13,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,7,12,18	8,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,7,12,16,17	8,11,13,15,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,7,12,14,17,18	8,11,13,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,7,12,14,16	8,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,7,12,14,17	8,11,13,15,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,7,12,14,16,18	8,11,13,15,18	$2^{-17.5}$

Table 0.1371 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,7,10	8	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,7,10,16,17,18	8,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,7,10,18	8,15,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,7,10,16,17	8,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,7,10,14,17,18	8,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,7,10,14,16	8	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,7,10,14,17	8,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,7,10,14,16,18	8,15,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,7,10,18	8,13,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,7,10,16,17	8,13,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,7,10	8,13,15	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,7,10,16,17,18	8,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,7,10,14,17	8,13,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,7,10,14,16,18	8,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,7,10,14,17,18	8,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,7,10,14,16	8,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,7,10,12,17,18	8,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,7,10,12,16	8	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,7,10,12,17	8,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,7,10,12,16,18	8,15,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,12,14	8	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10,12,14,16,17,18	8,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,12,14,18	8,15,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10,12,14,16,17	8,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,7,10,12,17	8,13,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,7,10,12,16,18	8,13,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,7,10,12,17,18	8,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,7,10,12,16	8,13,15	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,12,14,18	8,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10,12,14,16,17	8,13,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,12,14	8,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10,12,14,16,17,18	8,13,15,17,18	2^{-12}

Table 0.1372 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,7,10,18	8,11,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,7,10,16,17	8,11,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,7,10	8,11,15	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,7,10,16,17,18	8,11,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,7,10,14,17	8,11,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,7,10,14,16,18	8,11,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,7,10,14,17,18	8,11,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,7,10,14,16	8,11,15	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,7,10	8,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,7,10,16,17,18	8,11,13,17,18	2^{-1}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,7,10,18	8,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,7,10,16,17	8,11,13,15,17	2^{-1}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,7,10,14,17,18	8,11,13,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,7,10,14,16	8,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,7,10,14,17	8,11,13,15,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,7,10,14,16,18	8,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,7,10,12,17	8,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,7,10,12,16,18	8,11,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,7,10,12,17,18	8,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,7,10,12,16	8,11,15	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7,10,12,14,18	8,11,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,7,10,12,14,16,17	8,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7,10,12,14	8,11,15	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,7,10,12,14,16,17,18	8,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,7,10,12,17,18	8,11,13,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,7,10,12,16	8,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,7,10,12,17	8,11,13,15,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,7,10,12,16,18	8,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,7,10,12,14	8,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,7,10,12,14,16,17,18	8,11,13,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,7,10,12,14,18	8,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,7,10,12,14,16,17	8,11,13,15,17	2^{-12}

Table 0.1373 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,7,17	8,9,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,16,18	8,9,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,7,17,18	8,9,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,16	8,9,15	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,14,18	8,9,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,7,14,16,17	8,9,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,14	8,9,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,7,14,16,17,18	8,9,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,7,17,18	8,9,13,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,7,16	8,9,13	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,7,17	8,9,13,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,7,16,18	8,9,13,15,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,7,14	8,9,13	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,7,14,16,17,18	8,9,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,7,14,18	8,9,13,15,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,7,14,16,17	8,9,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,7,12,18	8,9,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,7,12,16,17	8,9,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,7,12	8,9,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,7,12,16,17,18	8,9,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,7,12,14,17	8,9,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,7,12,14,16,18	8,9,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,7,12,14,17,18	8,9,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,7,12,14,16	8,9,15	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,7,12	8,9,13	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,7,12,16,17,18	8,9,13,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,7,12,18	8,9,13,15,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,7,12,16,17	8,9,13,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,7,12,14,17,18	8,9,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,7,12,14,16	8,9,13	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,7,12,14,17	8,9,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,7,12,14,16,18	8,9,13,15,18	2^{-12}

Table 0.1374 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,7,17,18	8,9,11,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,7,16	8,9,11	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,7,17	8,9,11,15,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,7,16,18	8,9,11,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,7,14	8,9,11	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,7,14,16,17,18	8,9,11,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,7,14,18	8,9,11,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,7,14,16,17	8,9,11,15,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,7,17	8,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,7,16,18	8,9,11,13,18	2^{-1}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,7,17,18	8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,7,16	8,9,11,13,15	2^{-1}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,7,14,18	8,9,11,13,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,14,16,17	8,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,7,14	8,9,11,13,15	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,14,16,17,18	8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,7,12	8,9,11	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,7,12,16,17,18	8,9,11,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,7,12,18	8,9,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,7,12,16,17	8,9,11,15,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,7,12,14,17,18	8,9,11,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,7,12,14,16	8,9,11	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,7,12,14,17	8,9,11,15,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,7,12,14,16,18	8,9,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,7,12,18	8,9,11,13,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,7,12,16,17	8,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,7,12	8,9,11,13,15	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,7,12,16,17,18	8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,7,12,14,17	8,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,7,12,14,16,18	8,9,11,13,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,7,12,14,17,18	8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,7,12,14,16	8,9,11,13,15	2^{-12}

Table 0.1375 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,7,10,18	8,9,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,7,10,16,17	8,9,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7,10	8,9,15	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,7,10,16,17,18	8,9,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,7,10,14,17	8,9,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,7,10,14,16,18	8,9,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,7,10,14,17,18	8,9,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,7,10,14,16	8,9,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,7,10	8,9,13	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,7,10,16,17,18	8,9,13,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,7,10,18	8,9,13,15,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,7,10,16,17	8,9,13,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,7,10,14,17,18	8,9,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,7,10,14,16	8,9,13	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,7,10,14,17	8,9,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,7,10,14,16,18	8,9,13,15,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,7,10,12,17	8,9,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,7,10,12,16,18	8,9,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,7,10,12,17,18	8,9,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,7,10,12,16	8,9,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,7,10,12,14,18	8,9,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,7,10,12,14,16,17	8,9,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,7,10,12,14	8,9,15	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,7,10,12,14,16,17,18	8,9,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,7,10,12,17,18	8,9,13,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,7,10,12,16	8,9,13	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,7,10,12,17	8,9,13,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,7,10,12,16,18	8,9,13,15,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,7,10,12,14	8,9,13	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,7,10,12,14,16,17,18	8,9,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,7,10,12,14,18	8,9,13,15,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,7,10,12,14,16,17	8,9,13,15,17	$2^{-17.5}$

Table 0.1376 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,7,10	8,9,11	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,7,10,16,17,18	8,9,11,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,7,10,18	8,9,11,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,7,10,16,17	8,9,11,15,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,7,10,14,17,18	8,9,11,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,7,10,14,16	8,9,11	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,7,10,14,17	8,9,11,15,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,7,10,14,16,18	8,9,11,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,7,10,18	8,9,11,13,18	2^{-34}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,7,10,16,17	8,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,7,10	8,9,11,13,15	2^{-34}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,7,10,16,17,18	8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,7,10,14,17	8,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,7,10,14,16,18	8,9,11,13,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,7,10,14,17,18	8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,7,10,14,16	8,9,11,13,15	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,7,10,12,17,18	8,9,11,17,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,7,10,12,16	8,9,11	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,7,10,12,17	8,9,11,15,17	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,7,10,12,16,18	8,9,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,7,10,12,14	8,9,11	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,7,10,12,14,16,17,18	8,9,11,17,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,7,10,12,14,18	8,9,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,7,10,12,14,16,17	8,9,11,15,17	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,7,10,12,17	8,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,7,10,12,16,18	8,9,11,13,18	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,7,10,12,17,18	8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,7,10,12,16	8,9,11,13,15	2^{-12}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7,10,12,14,18	8,9,11,13,18	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,7,10,12,14,16,17	8,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7,10,12,14	8,9,11,13,15	2^{-23}
$(1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,7,10,12,14,16,17,18	8,9,11,13,15,17,18	$2^{-17.5}$

Table 0.1377 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,17	6,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,16,18	6,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,17,18	6,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,16	6,15	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,14,18	6,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,14,16,17	6,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,14	6,15	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,14,16,17,18	6,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,17,18	6,13,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,16	6,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,17	6,13,15,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,16,18	6,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,14	6,13	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,14,16,17,18	6,13,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,14,18	6,13,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,14,16,17	6,13,15,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,12,18	6,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,12,16,17	6,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,12	6,15	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,12,16,17,18	6,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,12,14,17	6,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,12,14,16,18	6,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,12,14,17,18	6,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,12,14,16	6,15	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,12	6,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,12,16,17,18	6,13,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,12,18	6,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,12,16,17	6,13,15,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,12,14,17,18	6,13,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,12,14,16	6,13	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,12,14,17	6,13,15,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,12,14,16,18	6,13,15,18	$2^{-28.5}$

Table 0.1378 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,17,18	6,11,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,16	6,11	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,17	6,11,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,16,18	6,11,15,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,14	6,11	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,14,16,17,18	6,11,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,14,18	6,11,15,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,14,16,17	6,11,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,17	6,11,13,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,16,18	6,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,17,18	6,11,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,16	6,11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,14,18	6,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,14,16,17	6,11,13,17	2^{-34}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,14	6,11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,14,16,17,18	6,11,13,15,17,18	2^{-34}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,12	6,11	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,12,16,17,18	6,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,12,18	6,11,15,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,12,16,17	6,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,12,14,17,18	6,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,12,14,16	6,11	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,12,14,17	6,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,12,14,16,18	6,11,15,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,12,18	6,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,12,16,17	6,11,13,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,12	6,11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,12,16,17,18	6,11,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,12,14,17	6,11,13,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,12,14,16,18	6,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,12,14,17,18	6,11,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,12,14,16	6,11,13,15	$2^{-17.5}$

Table 0.1379 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,10,18	6,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,10,16,17	6,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,10	6,15	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,10,16,17,18	6,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,10,14,17	6,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,10,14,16,18	6,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,10,14,17,18	6,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,10,14,16	6,15	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,10	6,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,10,16,17,18	6,13,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,10,18	6,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,10,16,17	6,13,15,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,10,14,17,18	6,13,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,10,14,16	6,13	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,10,14,17	6,13,15,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,10,14,16,18	6,13,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,10,12,17	6,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,10,12,16,18	6,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,10,12,17,18	6,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,10,12,16	6,15	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,10,12,14,18	6,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,10,12,14,16,17	6,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,10,12,14	6,15	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,10,12,14,16,17,18	6,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,10,12,17,18	6,13,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,10,12,16	6,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,10,12,17	6,13,15,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,10,12,16,18	6,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,10,12,14	6,13	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,10,12,14,16,17,18	6,13,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,10,12,14,18	6,13,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,10,12,14,16,17	6,13,15,17	2^{-12}

Table 0.1380 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,10	6,11	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,10,16,17,18	6,11,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,10,18	6,11,15,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,10,16,17	6,11,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,10,14,17,18	6,11,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,10,14,16	6,11	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,10,14,17	6,11,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,10,14,16,18	6,11,15,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,10,18	6,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,10,16,17	6,11,13,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,10	6,11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,10,16,17,18	6,11,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,10,14,17	6,11,13,17	2^{-1}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,10,14,16,18	6,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,10,14,17,18	6,11,13,15,17,18	2^{-1}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,10,14,16	6,11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,10,12,17,18	6,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,10,12,16	6,11	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,10,12,17	6,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,10,12,16,18	6,11,15,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,10,12,14	6,11	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,10,12,14,16,17,18	6,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,10,12,14,18	6,11,15,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,10,12,14,16,17	6,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,10,12,17	6,11,13,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,10,12,16,18	6,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,10,12,17,18	6,11,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,10,12,16	6,11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,10,12,14,18	6,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,10,12,14,16,17	6,11,13,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,10,12,14	6,11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,10,12,14,16,17,18	6,11,13,15,17,18	2^{-23}

Table 0.1381 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,17,18	6,9,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,16	6,9	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,17	6,9,15,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,16,18	6,9,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,14	6,9	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,14,16,17,18	6,9,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,14,18	6,9,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,14,16,17	6,9,15,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,17	6,9,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,16,18	6,9,13,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,17,18	6,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,16	6,9,13,15	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,14,18	6,9,13,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,14,16,17	6,9,13,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,14	6,9,13,15	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,14,16,17,18	6,9,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,12	6,9	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,12,16,17,18	6,9,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,12,18	6,9,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,12,16,17	6,9,15,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,12,14,17,18	6,9,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,12,14,16	6,9	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,12,14,17	6,9,15,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,12,14,16,18	6,9,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,12,18	6,9,13,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,12,16,17	6,9,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,12	6,9,13,15	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,12,16,17,18	6,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,12,14,17	6,9,13,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,12,14,16,18	6,9,13,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,12,14,17,18	6,9,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,12,14,16	6,9,13,15	2^{-12}

Table 0.1382 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,17	6,9,11,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,16,18	6,9,11,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,17,18	6,9,11,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,16	6,9,11,15	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,14,18	6,9,11,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,14,16,17	6,9,11,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,14	6,9,11,15	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,14,16,17,18	6,9,11,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,17,18	6,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,16	6,9,11,13	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,17	6,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,16,18	6,9,11,13,15,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,14	6,9,11,13	2^{-1}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,14,16,17,18	6,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,14,18	6,9,11,13,15,18	2^{-1}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,14,16,17	6,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,12,18	6,9,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,12,16,17	6,9,11,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,12	6,9,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,12,16,17,18	6,9,11,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,12,14,17	6,9,11,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,12,14,16,18	6,9,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,12,14,17,18	6,9,11,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,12,14,16	6,9,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,12	6,9,11,13	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,12,16,17,18	6,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,12,18	6,9,11,13,15,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,12,16,17	6,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,12,14,17,18	6,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,12,14,16	6,9,11,13	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,12,14,17	6,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,12,14,16,18	6,9,11,13,15,18	2^{-23}

Table 0.1383 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,10	6,9	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,10,16,17,18	6,9,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,10,18	6,9,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,10,16,17	6,9,15,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,10,14,17,18	6,9,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,10,14,16	6,9	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,10,14,17	6,9,15,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,10,14,16,18	6,9,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,10,18	6,9,13,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,10,16,17	6,9,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,10	6,9,13,15	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,10,16,17,18	6,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,10,14,17	6,9,13,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,10,14,16,18	6,9,13,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,10,14,17,18	6,9,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,10,14,16	6,9,13,15	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,10,12,17,18	6,9,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,10,12,16	6,9	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,10,12,17	6,9,15,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,10,12,16,18	6,9,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,10,12,14	6,9	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,10,12,14,16,17,18	6,9,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,10,12,14,18	6,9,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,10,12,14,16,17	6,9,15,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,10,12,17	6,9,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,10,12,16,18	6,9,13,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,10,12,17,18	6,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,10,12,16	6,9,13,15	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,10,12,14,18	6,9,13,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,10,12,14,16,17	6,9,13,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,10,12,14	6,9,13,15	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,10,12,14,16,17,18	6,9,13,15,17,18	$2^{-28.5}$

Table 0.1384 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,10,18	6,9,11,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,10,16,17	6,9,11,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,10	6,9,11,15	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,10,16,17,18	6,9,11,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,10,14,17	6,9,11,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,10,14,16,18	6,9,11,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,10,14,17,18	6,9,11,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,10,14,16	6,9,11,15	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,10	6,9,11,13	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,10,16,17,18	6,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,10,18	6,9,11,13,15,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,10,16,17	6,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,10,14,17,18	6,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,10,14,16	6,9,11,13	2^{-34}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,10,14,17	6,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,10,14,16,18	6,9,11,13,15,18	2^{-34}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,10,12,17	6,9,11,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,10,12,16,18	6,9,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,10,12,17,18	6,9,11,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,10,12,16	6,9,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,10,12,14,18	6,9,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,10,12,14,16,17	6,9,11,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,10,12,14	6,9,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,10,12,14,16,17,18	6,9,11,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,10,12,17,18	6,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,10,12,16	6,9,11,13	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,10,12,17	6,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,10,12,16,18	6,9,11,13,15,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,10,12,14	6,9,11,13	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,10,12,14,16,17,18	6,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,10,12,14,18	6,9,11,13,15,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,10,12,14,16,17	6,9,11,13,15,17	$2^{-17.5}$

Table 0.1385 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,18	6,8,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,16,17	6,8,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,5	6,8,15	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,16,17,18	6,8,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,14,17	6,8,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,14,16,18	6,8,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,14,17,18	6,8,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,14,16	6,8,15	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,5	6,8,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,16,17,18	6,8,13,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,18	6,8,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,16,17	6,8,13,15,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,14,17,18	6,8,13,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,14,16	6,8,13	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,14,17	6,8,13,15,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,14,16,18	6,8,13,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,12,17	6,8,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,12,16,18	6,8,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,12,17,18	6,8,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,12,16	6,8,15	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,12,14,18	6,8,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,12,14,16,17	6,8,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,12,14	6,8,15	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,12,14,16,17,18	6,8,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,12,17,18	6,8,13,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,12,16	6,8,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,12,17	6,8,13,15,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,12,16,18	6,8,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,12,14	6,8,13	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,12,14,16,17,18	6,8,13,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,12,14,18	6,8,13,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,12,14,16,17	6,8,13,15,17	2^{-23}

Table 0.1386 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,5	6,8,11	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,16,17,18	6,8,11,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,18	6,8,11,15,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,16,17	6,8,11,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,14,17,18	6,8,11,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,14,16	6,8,11	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,14,17	6,8,11,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,14,16,18	6,8,11,15,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,18	6,8,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,16,17	6,8,11,13,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,5	6,8,11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,16,17,18	6,8,11,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,14,17	6,8,11,13,17	2^{-34}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,14,16,18	6,8,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,14,17,18	6,8,11,13,15,17,18	2^{-34}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,14,16	6,8,11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,12,17,18	6,8,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,12,16	6,8,11	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,12,17	6,8,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,12,16,18	6,8,11,15,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,12,14	6,8,11	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,12,14,16,17,18	6,8,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,12,14,18	6,8,11,15,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,12,14,16,17	6,8,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,12,17	6,8,11,13,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,12,16,18	6,8,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,12,17,18	6,8,11,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,12,16	6,8,11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,12,14,18	6,8,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,12,14,16,17	6,8,11,13,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,12,14	6,8,11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,12,14,16,17,18	6,8,11,13,15,17,18	2^{-12}

Table 0.1387 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,10,17	6,8,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,10,16,18	6,8,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,10,17,18	6,8,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,10,16	6,8,15	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,10,14,18	6,8,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,10,14,16,17	6,8,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,10,14	6,8,15	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,10,14,16,17,18	6,8,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,10,17,18	6,8,13,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,10,16	6,8,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,10,17	6,8,13,15,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,10,16,18	6,8,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,10,14	6,8,13	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,10,14,16,17,18	6,8,13,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,10,14,18	6,8,13,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,10,14,16,17	6,8,13,15,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,10,12,18	6,8,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,10,12,16,17	6,8,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,10,12	6,8,15	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,10,12,16,17,18	6,8,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,10,12,14,17	6,8,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,10,12,14,16,18	6,8,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,10,12,14,17,18	6,8,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,10,12,14,16	6,8,15	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,10,12	6,8,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,10,12,16,17,18	6,8,13,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,10,12,18	6,8,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,10,12,16,17	6,8,13,15,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,10,12,14,17,18	6,8,13,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,10,12,14,16	6,8,13	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,10,12,14,17	6,8,13,15,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,10,12,14,16,18	6,8,13,15,18	$2^{-6.5}$

Table 0.1388 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,10,17,18	6,8,11,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,10,16	6,8,11	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,10,17	6,8,11,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,10,16,18	6,8,11,15,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,10,14	6,8,11	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,10,14,16,17,18	6,8,11,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,10,14,18	6,8,11,15,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,10,14,16,17	6,8,11,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,10,17	6,8,11,13,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,10,16,18	6,8,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,10,17,18	6,8,11,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,10,16	6,8,11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,10,14,18	6,8,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,10,14,16,17	6,8,11,13,17	2^{-1}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,10,14	6,8,11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,10,14,16,17,18	6,8,11,13,15,17,18	2^{-1}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,10,12	6,8,11	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,10,12,16,17,18	6,8,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,10,12,18	6,8,11,15,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,10,12,16,17	6,8,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,10,12,14,17,18	6,8,11,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,10,12,14,16	6,8,11	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,10,12,14,17	6,8,11,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,10,12,14,16,18	6,8,11,15,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,10,12,18	6,8,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,10,12,16,17	6,8,11,13,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,10,12	6,8,11,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,10,12,16,17,18	6,8,11,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,10,12,14,17	6,8,11,13,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,10,12,14,16,18	6,8,11,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,10,12,14,17,18	6,8,11,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,10,12,14,16	6,8,11,13,15	$2^{-17.5}$

Table 0.1389 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,5	6,8,9	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,16,17,18	6,8,9,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,18	6,8,9,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,16,17	6,8,9,15,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,14,17,18	6,8,9,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,14,16	6,8,9	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,14,17	6,8,9,15,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,14,16,18	6,8,9,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,18	6,8,9,13,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,16,17	6,8,9,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,5	6,8,9,13,15	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,16,17,18	6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,14,17	6,8,9,13,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,14,16,18	6,8,9,13,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,14,17,18	6,8,9,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,14,16	6,8,9,13,15	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,12,17,18	6,8,9,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,12,16	6,8,9	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,12,17	6,8,9,15,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,12,16,18	6,8,9,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,12,14	6,8,9	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,12,14,16,17,18	6,8,9,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,12,14,18	6,8,9,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,12,14,16,17	6,8,9,15,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,12,17	6,8,9,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,12,16,18	6,8,9,13,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,12,17,18	6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,12,16	6,8,9,13,15	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,12,14,18	6,8,9,13,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,12,14,16,17	6,8,9,13,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,12,14	6,8,9,13,15	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,12,14,16,17,18	6,8,9,13,15,17,18	$2^{-6.5}$

Table 0.1390 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,18	6,8,9,11,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,16,17	6,8,9,11,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,5	6,8,9,11,15	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,16,17,18	6,8,9,11,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,14,17	6,8,9,11,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,14,16,18	6,8,9,11,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,14,17,18	6,8,9,11,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,14,16	6,8,9,11,15	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,5	6,8,9,11,13	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,16,17,18	6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,18	6,8,9,11,13,15,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,16,17	6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,14,17,18	6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,14,16	6,8,9,11,13	2^{-1}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,14,17	6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,14,16,18	6,8,9,11,13,15,18	2^{-1}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,12,17	6,8,9,11,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,12,16,18	6,8,9,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,12,17,18	6,8,9,11,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,12,16	6,8,9,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,12,14,18	6,8,9,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,12,14,16,17	6,8,9,11,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,12,14	6,8,9,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,12,14,16,17,18	6,8,9,11,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,12,17,18	6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,12,16	6,8,9,11,13	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,12,17	6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,12,16,18	6,8,9,11,13,15,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,12,14	6,8,9,11,13	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,12,14,16,17,18	6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,12,14,18	6,8,9,11,13,15,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,12,14,16,17	6,8,9,11,13,15,17	$2^{-17.5}$

Table 0.1391 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,10,17,18	6,8,9,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,10,16	6,8,9	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,10,17	6,8,9,15,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,10,16,18	6,8,9,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,10,14	6,8,9	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,10,14,16,17,18	6,8,9,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,10,14,18	6,8,9,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,10,14,16,17	6,8,9,15,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,10,17	6,8,9,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,10,16,18	6,8,9,13,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,10,17,18	6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,10,16	6,8,9,13,15	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,10,14,18	6,8,9,13,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,10,14,16,17	6,8,9,13,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,10,14	6,8,9,13,15	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,10,14,16,17,18	6,8,9,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,10,12	6,8,9	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,10,12,16,17,18	6,8,9,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,10,12,18	6,8,9,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,10,12,16,17	6,8,9,15,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,10,12,14,17,18	6,8,9,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,10,12,14,16	6,8,9	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,10,12,14,17	6,8,9,15,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,10,12,14,16,18	6,8,9,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,10,12,18	6,8,9,13,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,10,12,16,17	6,8,9,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,10,12	6,8,9,13,15	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,10,12,16,17,18	6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,10,12,14,17	6,8,9,13,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,10,12,14,16,18	6,8,9,13,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,10,12,14,17,18	6,8,9,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,10,12,14,16	6,8,9,13,15	2^{-23}

Table 0.1392 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,10,17	6,8,9,11,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,10,16,18	6,8,9,11,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,10,17,18	6,8,9,11,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,10,16	6,8,9,11,15	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,10,14,18	6,8,9,11,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,10,14,16,17	6,8,9,11,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,10,14	6,8,9,11,15	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,10,14,16,17,18	6,8,9,11,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,10,17,18	6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,10,16	6,8,9,11,13	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,10,17	6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,10,16,18	6,8,9,11,13,15,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,10,14	6,8,9,11,13	2^{-34}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,10,14,16,17,18	6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,10,14,18	6,8,9,11,13,15,18	2^{-34}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,10,14,16,17	6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,10,12,18	6,8,9,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,10,12,16,17	6,8,9,11,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,10,12	6,8,9,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,10,12,16,17,18	6,8,9,11,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,10,12,14,17	6,8,9,11,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,10,12,14,16,18	6,8,9,11,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,10,12,14,17,18	6,8,9,11,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,10,12,14,16	6,8,9,11,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,10,12	6,8,9,11,13	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,10,12,16,17,18	6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,10,12,18	6,8,9,11,13,15,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,10,12,16,17	6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,10,12,14,17,18	6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,10,12,14,16	6,8,9,11,13	2^{-12}
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,10,12,14,17	6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,10,12,14,16,18	6,8,9,11,13,15,18	2^{-12}

Table 0.1393 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,7,17,18	6,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,7,16	6	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,7,17	6,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,7,16,18	6,15,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,7,14	6	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,7,14,16,17,18	6,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,7,14,18	6,15,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,7,14,16,17	6,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,7,17	6,13,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,7,16,18	6,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,7,17,18	6,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,7,16	6,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,7,14,18	6,13,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,7,14,16,17	6,13,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,7,14	6,13,15	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,7,14,16,17,18	6,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,7,12	6	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,12,16,17,18	6,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,7,12,18	6,15,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,12,16,17	6,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,12,14,17,18	6,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,7,12,14,16	6	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,12,14,17	6,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,7,12,14,16,18	6,15,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,7,12,18	6,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,7,12,16,17	6,13,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,7,12	6,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,7,12,16,17,18	6,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,7,12,14,17	6,13,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,7,12,14,16,18	6,13,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,7,12,14,17,18	6,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,7,12,14,16	6,13,15	$2^{-28.5}$

Table 0.1394 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,7,17	6,11,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,7,16,18	6,11,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,7,17,18	6,11,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,7,16	6,11,15	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,7,14,18	6,11,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,7,14,16,17	6,11,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,7,14	6,11,15	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,7,14,16,17,18	6,11,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,7,17,18	6,11,13,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,7,16	6,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,7,17	6,11,13,15,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,7,16,18	6,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,7,14	6,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,7,14,16,17,18	6,11,13,17,18	2^{-34}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,7,14,18	6,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,7,14,16,17	6,11,13,15,17	2^{-34}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,7,12,18	6,11,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,7,12,16,17	6,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,7,12	6,11,15	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,7,12,16,17,18	6,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,7,12,14,17	6,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,7,12,14,16,18	6,11,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,7,12,14,17,18	6,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,7,12,14,16	6,11,15	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,12	6,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,7,12,16,17,18	6,11,13,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,12,18	6,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,7,12,16,17	6,11,13,15,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,7,12,14,17,18	6,11,13,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,7,12,14,16	6,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,7,12,14,17	6,11,13,15,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,7,12,14,16,18	6,11,13,15,18	$2^{-17.5}$

Table 0.1395 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,7,10	6	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,7,10,16,17,18	6,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,7,10,18	6,15,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,7,10,16,17	6,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,7,10,14,17,18	6,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,7,10,14,16	6	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,7,10,14,17	6,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,7,10,14,16,18	6,15,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,7,10,18	6,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,7,10,16,17	6,13,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,7,10	6,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,7,10,16,17,18	6,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,7,10,14,17	6,13,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,7,10,14,16,18	6,13,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,7,10,14,17,18	6,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,7,10,14,16	6,13,15	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,7,10,12,17,18	6,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,7,10,12,16	6	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,7,10,12,17	6,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,7,10,12,16,18	6,15,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,7,10,12,14	6	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,7,10,12,14,16,17,18	6,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,7,10,12,14,18	6,15,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,7,10,12,14,16,17	6,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,7,10,12,17	6,13,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,7,10,12,16,18	6,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,7,10,12,17,18	6,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,7,10,12,16	6,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,7,10,12,14,18	6,13,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,7,10,12,14,16,17	6,13,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,7,10,12,14	6,13,15	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,7,10,12,14,16,17,18	6,13,15,17,18	2^{-12}

Table 0.1396 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,7,10,18	6,11,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,7,10,16,17	6,11,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,7,10	6,11,15	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,7,10,16,17,18	6,11,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,7,10,14,17	6,11,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,7,10,14,16,18	6,11,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,7,10,14,17,18	6,11,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,7,10,14,16	6,11,15	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,7,10	6,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7,10,16,17,18	6,11,13,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,7,10,18	6,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7,10,16,17	6,11,13,15,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,7,10,14,17,18	6,11,13,17,18	2^{-1}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,7,10,14,16	6,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,7,10,14,17	6,11,13,15,17	2^{-1}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,7,10,14,16,18	6,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,7,10,12,17	6,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,7,10,12,16,18	6,11,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,7,10,12,17,18	6,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,7,10,12,16	6,11,15	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,7,10,12,14,18	6,11,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,7,10,12,14,16,17	6,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,7,10,12,14	6,11,15	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7,10,12,14,16,17,18	6,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,7,10,12,17,18	6,11,13,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,7,10,12,16	6,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,7,10,12,17	6,11,13,15,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,7,10,12,16,18	6,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,7,10,12,14	6,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,7,10,12,14,16,17,18	6,11,13,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,7,10,12,14,18	6,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,7,10,12,14,16,17	6,11,13,15,17	2^{-23}

Table 0.1397 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,7,17	6,9,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,7,16,18	6,9,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,7,17,18	6,9,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,7,16	6,9,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,7,14,18	6,9,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,7,14,16,17	6,9,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,7,14	6,9,15	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,7,14,16,17,18	6,9,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,7,17,18	6,9,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,7,16	6,9,13	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,7,17	6,9,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,7,16,18	6,9,13,15,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,7,14	6,9,13	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,7,14,16,17,18	6,9,13,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,7,14,18	6,9,13,15,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,7,14,16,17	6,9,13,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,7,12,18	6,9,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,7,12,16,17	6,9,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,7,12	6,9,15	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,7,12,16,17,18	6,9,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,7,12,14,17	6,9,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,7,12,14,16,18	6,9,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,7,12,14,17,18	6,9,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,7,12,14,16	6,9,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,7,12	6,9,13	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,7,12,16,17,18	6,9,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,7,12,18	6,9,13,15,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,7,12,16,17	6,9,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,7,12,14,17,18	6,9,13,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,7,12,14,16	6,9,13	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,7,12,14,17	6,9,13,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,7,12,14,16,18	6,9,13,15,18	2^{-12}

Table 0.1398 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,7,17,18	6,9,11,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,7,16	6,9,11	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,7,17	6,9,11,15,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,7,16,18	6,9,11,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,7,14	6,9,11	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,7,14,16,17,18	6,9,11,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,7,14,18	6,9,11,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,7,14,16,17	6,9,11,15,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,7,17	6,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,7,16,18	6,9,11,13,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,7,17,18	6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,7,16	6,9,11,13,15	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,7,14,18	6,9,11,13,18	2^{-1}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,7,14,16,17	6,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,7,14	6,9,11,13,15	2^{-1}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,7,14,16,17,18	6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,7,12	6,9,11	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,7,12,16,17,18	6,9,11,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,7,12,18	6,9,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,7,12,16,17	6,9,11,15,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,7,12,14,17,18	6,9,11,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,7,12,14,16	6,9,11	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,7,12,14,17	6,9,11,15,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,7,12,14,16,18	6,9,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,7,12,18	6,9,11,13,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,7,12,16,17	6,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,7,12	6,9,11,13,15	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,7,12,16,17,18	6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,7,12,14,17	6,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,7,12,14,16,18	6,9,11,13,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,7,12,14,17,18	6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,7,12,14,16	6,9,11,13,15	2^{-23}

Table 0.1399 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10,18	6,9,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,16,17	6,9,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10	6,9,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,16,17,18	6,9,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,7,10,14,17	6,9,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,7,10,14,16,18	6,9,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,7,10,14,17,18	6,9,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,7,10,14,16	6,9,15	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10	6,9,13	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,16,17,18	6,9,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10,18	6,9,13,15,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,16,17	6,9,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,7,10,14,17,18	6,9,13,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,7,10,14,16	6,9,13	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,7,10,14,17	6,9,13,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,7,10,14,16,18	6,9,13,15,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,7,10,12,17	6,9,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,7,10,12,16,18	6,9,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,7,10,12,17,18	6,9,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,7,10,12,16	6,9,15	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,7,10,12,14,18	6,9,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,7,10,12,14,16,17	6,9,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,7,10,12,14	6,9,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,12,14,16,17,18	6,9,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,7,10,12,17,18	6,9,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,7,10,12,16	6,9,13	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,7,10,12,17	6,9,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,7,10,12,16,18	6,9,13,15,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,7,10,12,14	6,9,13	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,7,10,12,14,16,17,18	6,9,13,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,7,10,12,14,18	6,9,13,15,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,7,10,12,14,16,17	6,9,13,15,17	$2^{-28.5}$

Table 0.1400 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,7,10	6,9,11	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7,10,16,17,18	6,9,11,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,7,10,18	6,9,11,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7,10,16,17	6,9,11,15,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,7,10,14,17,18	6,9,11,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,7,10,14,16	6,9,11	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,7,10,14,17	6,9,11,15,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,7,10,14,16,18	6,9,11,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,7,10,18	6,9,11,13,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,7,10,16,17	6,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,7,10	6,9,11,13,15	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,7,10,16,17,18	6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,7,10,14,17	6,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,7,10,14,16,18	6,9,11,13,18	2^{-34}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,7,10,14,17,18	6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,7,10,14,16	6,9,11,13,15	2^{-34}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,7,10,12,17,18	6,9,11,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,7,10,12,16	6,9,11	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,7,10,12,17	6,9,11,15,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,7,10,12,16,18	6,9,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,7,10,12,14	6,9,11	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,7,10,12,14,16,17,18	6,9,11,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,7,10,12,14,18	6,9,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,7,10,12,14,16,17	6,9,11,15,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,7,10,12,17	6,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,7,10,12,16,18	6,9,11,13,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,7,10,12,17,18	6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,7,10,12,16	6,9,11,13,15	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,7,10,12,14,18	6,9,11,13,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,7,10,12,14,16,17	6,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,7,10,12,14	6,9,11,13,15	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,7,10,12,14,16,17,18	6,9,11,13,15,17,18	$2^{-17.5}$

Table 0.1401 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,7	6,8	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,7,16,17,18	6,8,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,7,18	6,8,15,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,7,16,17	6,8,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7,14,17,18	6,8,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,7,14,16	6,8	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7,14,17	6,8,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,7,14,16,18	6,8,15,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,7,18	6,8,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,7,16,17	6,8,13,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,7	6,8,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,7,16,17,18	6,8,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7,14,17	6,8,13,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,7,14,16,18	6,8,13,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7,14,17,18	6,8,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,7,14,16	6,8,13,15	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,7,12,17,18	6,8,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,7,12,16	6,8	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,7,12,17	6,8,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,7,12,16,18	6,8,15,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,7,12,14	6,8	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,7,12,14,16,17,18	6,8,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,7,12,14,18	6,8,15,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,7,12,14,16,17	6,8,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,7,12,17	6,8,13,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,7,12,16,18	6,8,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,7,12,17,18	6,8,13,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,7,12,16	6,8,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,7,12,14,18	6,8,13,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,7,12,14,16,17	6,8,13,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,7,12,14	6,8,13,15	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,7,12,14,16,17,18	6,8,13,15,17,18	2^{-23}

Table 0.1402 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7,18	6,8,11,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,7,16,17	6,8,11,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7	6,8,11,15	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,7,16,17,18	6,8,11,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,7,14,17	6,8,11,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,7,14,16,18	6,8,11,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,7,14,17,18	6,8,11,15,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,7,14,16	6,8,11,15	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,7	6,8,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,7,16,17,18	6,8,11,13,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,7,18	6,8,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,7,16,17	6,8,11,13,15,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,7,14,17,18	6,8,11,13,17,18	2^{-34}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,7,14,16	6,8,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,7,14,17	6,8,11,13,15,17	2^{-34}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,7,14,16,18	6,8,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,7,12,17	6,8,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,7,12,16,18	6,8,11,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,7,12,17,18	6,8,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,7,12,16	6,8,11,15	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,7,12,14,18	6,8,11,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,7,12,14,16,17	6,8,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,7,12,14	6,8,11,15	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,7,12,14,16,17,18	6,8,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,7,12,17,18	6,8,11,13,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,7,12,16	6,8,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,7,12,17	6,8,11,13,15,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,7,12,16,18	6,8,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,7,12,14	6,8,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,7,12,14,16,17,18	6,8,11,13,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,7,12,14,18	6,8,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,7,12,14,16,17	6,8,11,13,15,17	2^{-12}

Table 0.1403 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,7,10,17,18	6,8,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,7,10,16	6,8	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,7,10,17	6,8,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,7,10,16,18	6,8,15,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,7,10,14	6,8	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,7,10,14,16,17,18	6,8,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,7,10,14,18	6,8,15,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,7,10,14,16,17	6,8,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,7,10,17	6,8,13,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,7,10,16,18	6,8,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,7,10,17,18	6,8,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,7,10,16	6,8,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,7,10,14,18	6,8,13,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,7,10,14,16,17	6,8,13,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,7,10,14	6,8,13,15	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,7,10,14,16,17,18	6,8,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,7,10,12	6,8	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,7,10,12,16,17,18	6,8,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,7,10,12,18	6,8,15,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,7,10,12,16,17	6,8,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,7,10,12,14,17,18	6,8,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,7,10,12,14,16	6,8	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,7,10,12,14,17	6,8,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,7,10,12,14,16,18	6,8,15,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,7,10,12,18	6,8,13,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,7,10,12,16,17	6,8,13,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,7,10,12	6,8,13,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,7,10,12,16,17,18	6,8,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,7,10,12,14,17	6,8,13,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,7,10,12,14,16,18	6,8,13,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,7,10,12,14,17,18	6,8,13,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,7,10,12,14,16	6,8,13,15	$2^{-6.5}$

Table 0.1404 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,7,10,17	6,8,11,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,7,10,16,18	6,8,11,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,7,10,17,18	6,8,11,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,7,10,16	6,8,11,15	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,7,10,14,18	6,8,11,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,7,10,14,16,17	6,8,11,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,7,10,14	6,8,11,15	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,7,10,14,16,17,18	6,8,11,15,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,7,10,17,18	6,8,11,13,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,7,10,16	6,8,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,7,10,17	6,8,11,13,15,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,7,10,16,18	6,8,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,7,10,14	6,8,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,7,10,14,16,17,18	6,8,11,13,17,18	2^{-1}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,7,10,14,18	6,8,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,7,10,14,16,17	6,8,11,13,15,17	2^{-1}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,7,10,12,18	6,8,11,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,7,10,12,16,17	6,8,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,7,10,12	6,8,11,15	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,7,10,12,16,17,18	6,8,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,7,10,12,14,17	6,8,11,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,7,10,12,14,16,18	6,8,11,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,7,10,12,14,17,18	6,8,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,7,10,12,14,16	6,8,11,15	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,7,10,12	6,8,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,7,10,12,16,17,18	6,8,11,13,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,7,10,12,18	6,8,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,7,10,12,16,17	6,8,11,13,15,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,7,10,12,14,17,18	6,8,11,13,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,7,10,12,14,16	6,8,11,13	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,7,10,12,14,17	6,8,11,13,15,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,7,10,12,14,16,18	6,8,11,13,15,18	$2^{-17.5}$

Table 0.1405 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,7,18	6,8,9,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,7,16,17	6,8,9,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,7	6,8,9,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,7,16,17,18	6,8,9,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,7,14,17	6,8,9,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,7,14,16,18	6,8,9,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,7,14,17,18	6,8,9,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,7,14,16	6,8,9,15	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,7	6,8,9,13	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,7,16,17,18	6,8,9,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,7,18	6,8,9,13,15,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,7,16,17	6,8,9,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,7,14,17,18	6,8,9,13,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,7,14,16	6,8,9,13	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,7,14,17	6,8,9,13,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,7,14,16,18	6,8,9,13,15,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,7,12,17	6,8,9,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,7,12,16,18	6,8,9,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,7,12,17,18	6,8,9,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,7,12,16	6,8,9,15	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,7,12,14,18	6,8,9,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,7,12,14,16,17	6,8,9,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,7,12,14	6,8,9,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,7,12,14,16,17,18	6,8,9,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,7,12,17,18	6,8,9,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,7,12,16	6,8,9,13	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,7,12,17	6,8,9,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,7,12,16,18	6,8,9,13,15,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,7,12,14	6,8,9,13	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,7,12,14,16,17,18	6,8,9,13,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,7,12,14,18	6,8,9,13,15,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,7,12,14,16,17	6,8,9,13,15,17	$2^{-6.5}$

Table 0.1406 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,7	6,8,9,11	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,7,16,17,18	6,8,9,11,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,7,18	6,8,9,11,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,7,16,17	6,8,9,11,15,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,7,14,17,18	6,8,9,11,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,7,14,16	6,8,9,11	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,7,14,17	6,8,9,11,15,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,7,14,16,18	6,8,9,11,15,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7,18	6,8,9,11,13,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,7,16,17	6,8,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7	6,8,9,11,13,15	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,7,16,17,18	6,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,7,14,17	6,8,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,7,14,16,18	6,8,9,11,13,18	2^{-1}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,7,14,17,18	6,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,7,14,16	6,8,9,11,13,15	2^{-1}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,7,12,17,18	6,8,9,11,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,7,12,16	6,8,9,11	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,7,12,17	6,8,9,11,15,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,7,12,16,18	6,8,9,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,7,12,14	6,8,9,11	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,7,12,14,16,17,18	6,8,9,11,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,7,12,14,18	6,8,9,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,7,12,14,16,17	6,8,9,11,15,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,7,12,17	6,8,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,7,12,16,18	6,8,9,11,13,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,7,12,17,18	6,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,7,12,16	6,8,9,11,13,15	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,7,12,14,18	6,8,9,11,13,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,7,12,14,16,17	6,8,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,7,12,14	6,8,9,11,13,15	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,7,12,14,16,17,18	6,8,9,11,13,15,17,18	$2^{-17.5}$

Table 0.1407 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,7,10,17	6,8,9,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,7,10,16,18	6,8,9,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,7,10,17,18	6,8,9,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,7,10,16	6,8,9,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,7,10,14,18	6,8,9,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,14,16,17	6,8,9,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,7,10,14	6,8,9,15	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,14,16,17,18	6,8,9,15,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,7,10,17,18	6,8,9,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,7,10,16	6,8,9,13	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,7,10,17	6,8,9,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,7,10,16,18	6,8,9,13,15,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,7,10,14	6,8,9,13	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,14,16,17,18	6,8,9,13,17,18	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,7,10,14,18	6,8,9,13,15,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,14,16,17	6,8,9,13,15,17	$2^{-6.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,10,12,18	6,8,9,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,7,10,12,16,17	6,8,9,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,10,12	6,8,9,15	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,7,10,12,16,17,18	6,8,9,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,7,10,12,14,17	6,8,9,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,10,12,14,16,18	6,8,9,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,7,10,12,14,17,18	6,8,9,15,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,10,12,14,16	6,8,9,15	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,10,12	6,8,9,13	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,7,10,12,16,17,18	6,8,9,13,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,7,10,12,18	6,8,9,13,15,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,7,10,12,16,17	6,8,9,13,15,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,7,10,12,14,17,18	6,8,9,13,17,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,7,10,12,14,16	6,8,9,13	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,7,10,12,14,17	6,8,9,13,15,17	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,7,10,12,14,16,18	6,8,9,13,15,18	2^{-23}

Table 0.1408 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,7,10,17,18	6,8,9,11,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,7,10,16	6,8,9,11	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,7,10,17	6,8,9,11,15,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,7,10,16,18	6,8,9,11,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,7,10,14	6,8,9,11	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,7,10,14,16,17,18	6,8,9,11,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,7,10,14,18	6,8,9,11,15,18	$2^{-28.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,7,10,14,16,17	6,8,9,11,15,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,7,10,17	6,8,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,7,10,16,18	6,8,9,11,13,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,7,10,17,18	6,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,7,10,16	6,8,9,11,13,15	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,7,10,14,18	6,8,9,11,13,18	2^{-34}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,7,10,14,16,17	6,8,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,7,10,14	6,8,9,11,13,15	2^{-34}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,7,10,14,16,17,18	6,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,7,10,12	6,8,9,11	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,7,10,12,16,17,18	6,8,9,11,17,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,7,10,12,18	6,8,9,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,7,10,12,16,17	6,8,9,11,15,17	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,7,10,12,14,17,18	6,8,9,11,17,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,7,10,12,14,16	6,8,9,11	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,7,10,12,14,17	6,8,9,11,15,17	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,7,10,12,14,16,18	6,8,9,11,15,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,7,10,12,18	6,8,9,11,13,18	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,10,12,16,17	6,8,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,7,10,12	6,8,9,11,13,15	2^{-23}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,10,12,16,17,18	6,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,7,10,12,14,17	6,8,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,7,10,12,14,16,18	6,8,9,11,13,18	2^{-12}
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,7,10,12,14,17,18	6,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,7,10,12,14,16	6,8,9,11,13,15	2^{-12}

Table 0.1409 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,17,18	4,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,16	4	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,17	4,15,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,16,18	4,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,14	4	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,14,16,17,18	4,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,14,18	4,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,14,16,17	4,15,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,17	4,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,16,18	4,13,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,17,18	4,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,16	4,13,15	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,14,18	4,13,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,14,16,17	4,13,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,14	4,13,15	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,14,16,17,18	4,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,12	4	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,12,16,17,18	4,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,12,18	4,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,12,16,17	4,15,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,12,14,17,18	4,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,12,14,16	4	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,12,14,17	4,15,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,12,14,16,18	4,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,12,18	4,13,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,12,16,17	4,13,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,12	4,13,15	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,12,16,17,18	4,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,12,14,17	4,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,12,14,16,18	4,13,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,12,14,17,18	4,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,12,14,16	4,13,15	2^{-12}

Table 0.1410 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,17	4,11,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,16,18	4,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,17,18	4,11,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,16	4,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,14,18	4,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,14,16,17	4,11,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,14	4,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,14,16,17,18	4,11,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,17,18	4,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,16	4,11,13	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,17	4,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,16,18	4,11,13,15,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,14	4,11,13	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,14,16,17,18	4,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,14,18	4,11,13,15,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,14,16,17	4,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,12,18	4,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,12,16,17	4,11,17	2^{-34}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,12	4,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,12,16,17,18	4,11,15,17,18	2^{-34}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,12,14,17	4,11,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,12,14,16,18	4,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,12,14,17,18	4,11,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,12,14,16	4,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,12	4,11,13	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,12,16,17,18	4,11,13,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,12,18	4,11,13,15,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,12,16,17	4,11,13,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,12,14,17,18	4,11,13,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,12,14,16	4,11,13	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,12,14,17	4,11,13,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,12,14,16,18	4,11,13,15,18	2^{-23}

Table 0.1411 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,10	4	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,10,16,17,18	4,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,10,18	4,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,10,16,17	4,15,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,10,14,17,18	4,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,10,14,16	4	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,10,14,17	4,15,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,10,14,16,18	4,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,10,18	4,13,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,10,16,17	4,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,10	4,13,15	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,10,16,17,18	4,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,10,14,17	4,13,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,10,14,16,18	4,13,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,10,14,17,18	4,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,10,14,16	4,13,15	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,10,12,17,18	4,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,10,12,16	4	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,10,12,17	4,15,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,10,12,16,18	4,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,10,12,14	4	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,10,12,14,16,17,18	4,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,10,12,14,18	4,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,10,12,14,16,17	4,15,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,10,12,17	4,13,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,10,12,16,18	4,13,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,10,12,17,18	4,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,10,12,16	4,13,15	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,10,12,14,18	4,13,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,10,12,14,16,17	4,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,10,12,14	4,13,15	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,10,12,14,16,17,18	4,13,15,17,18	$2^{-17.5}$

Table 0.1412 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,10,18	4,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,10,16,17	4,11,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,10	4,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,10,16,17,18	4,11,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,10,14,17	4,11,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,10,14,16,18	4,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,10,14,17,18	4,11,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,10,14,16	4,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,10	4,11,13	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,10,16,17,18	4,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,10,18	4,11,13,15,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,10,16,17	4,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,10,14,17,18	4,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,10,14,16	4,11,13	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,10,14,17	4,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,10,14,16,18	4,11,13,15,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,10,12,17	4,11,17	2^{-1}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,10,12,16,18	4,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,10,12,17,18	4,11,15,17,18	2^{-1}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,10,12,16	4,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,10,12,14,18	4,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,10,12,14,16,17	4,11,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,10,12,14	4,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,10,12,14,16,17,18	4,11,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,10,12,17,18	4,11,13,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,10,12,16	4,11,13	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,10,12,17	4,11,13,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,10,12,16,18	4,11,13,15,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,10,12,14	4,11,13	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,10,12,14,16,17,18	4,11,13,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,10,12,14,18	4,11,13,15,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,10,12,14,16,17	4,11,13,15,17	$2^{-6.5}$

Table 0.1413 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,17	4,9,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,16,18	4,9,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,17,18	4,9,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,16	4,9,15	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,14,18	4,9,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,14,16,17	4,9,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,14	4,9,15	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,14,16,17,18	4,9,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,17,18	4,9,13,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,16	4,9,13	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,17	4,9,13,15,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,16,18	4,9,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,14	4,9,13	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,14,16,17,18	4,9,13,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,14,18	4,9,13,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,14,16,17	4,9,13,15,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,12,18	4,9,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,12,16,17	4,9,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,12	4,9,15	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,12,16,17,18	4,9,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,12,14,17	4,9,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,12,14,16,18	4,9,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,12,14,17,18	4,9,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,12,14,16	4,9,15	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,12	4,9,13	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,12,16,17,18	4,9,13,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,12,18	4,9,13,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,12,16,17	4,9,13,15,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,12,14,17,18	4,9,13,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,12,14,16	4,9,13	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,12,14,17	4,9,13,15,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,12,14,16,18	4,9,13,15,18	$2^{-17.5}$

Table 0.1414 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,17,18	4,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,16	4,9,11	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,17	4,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,16,18	4,9,11,15,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,14	4,9,11	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,14,16,17,18	4,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,14,18	4,9,11,15,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,14,16,17	4,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,17	4,9,11,13,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,16,18	4,9,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,17,18	4,9,11,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,16	4,9,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,14,18	4,9,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,14,16,17	4,9,11,13,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,14	4,9,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,14,16,17,18	4,9,11,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,12	4,9,11	2^{-1}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,12,16,17,18	4,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,12,18	4,9,11,15,18	2^{-1}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,12,16,17	4,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,12,14,17,18	4,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,12,14,16	4,9,11	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,12,14,17	4,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,12,14,16,18	4,9,11,15,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,12,18	4,9,11,13,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,12,16,17	4,9,11,13,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,12	4,9,11,13,15	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,12,16,17,18	4,9,11,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,12,14,17	4,9,11,13,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,12,14,16,18	4,9,11,13,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,12,14,17,18	4,9,11,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,12,14,16	4,9,11,13,15	$2^{-6.5}$

Table 0.1415 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,10,18	4,9,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,10,16,17	4,9,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,10	4,9,15	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,10,16,17,18	4,9,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,10,14,17	4,9,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,10,14,16,18	4,9,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,10,14,17,18	4,9,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,10,14,16	4,9,15	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,10	4,9,13	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,10,16,17,18	4,9,13,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,10,18	4,9,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,10,16,17	4,9,13,15,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,10,14,17,18	4,9,13,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,10,14,16	4,9,13	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,10,14,17	4,9,13,15,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,10,14,16,18	4,9,13,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,10,12,17	4,9,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,10,12,16,18	4,9,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,10,12,17,18	4,9,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,10,12,16	4,9,15	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,10,12,14,18	4,9,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,10,12,14,16,17	4,9,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,10,12,14	4,9,15	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,10,12,14,16,17,18	4,9,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,10,12,17,18	4,9,13,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,10,12,16	4,9,13	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,10,12,17	4,9,13,15,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,10,12,16,18	4,9,13,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,10,12,14	4,9,13	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,10,12,14,16,17,18	4,9,13,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,10,12,14,18	4,9,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,10,12,14,16,17	4,9,13,15,17	2^{-12}

Table 0.1416 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,10	4,9,11	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,10,16,17,18	4,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,10,18	4,9,11,15,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,10,16,17	4,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,10,14,17,18	4,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,10,14,16	4,9,11	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,10,14,17	4,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,10,14,16,18	4,9,11,15,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,10,18	4,9,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,10,16,17	4,9,11,13,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,10	4,9,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,10,16,17,18	4,9,11,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,10,14,17	4,9,11,13,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,10,14,16,18	4,9,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,10,14,17,18	4,9,11,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,10,14,16	4,9,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,10,12,17,18	4,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,10,12,16	4,9,11	2^{-34}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,10,12,17	4,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,10,12,16,18	4,9,11,15,18	2^{-34}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,10,12,14	4,9,11	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,10,12,14,16,17,18	4,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,10,12,14,18	4,9,11,15,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,10,12,14,16,17	4,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,10,12,17	4,9,11,13,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,10,12,16,18	4,9,11,13,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,10,12,17,18	4,9,11,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,10,12,16	4,9,11,13,15	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,10,12,14,18	4,9,11,13,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,10,12,14,16,17	4,9,11,13,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,10,12,14	4,9,11,13,15	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,10,12,14,16,17,18	4,9,11,13,15,17,18	2^{-23}

Table 0.1417 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3	4,8	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,16,17,18	4,8,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,18	4,8,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,16,17	4,8,15,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,14,17,18	4,8,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,14,16	4,8	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,14,17	4,8,15,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,14,16,18	4,8,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,18	4,8,13,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,16,17	4,8,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3	4,8,13,15	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,16,17,18	4,8,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,14,17	4,8,13,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,14,16,18	4,8,13,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,14,17,18	4,8,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,14,16	4,8,13,15	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,12,17,18	4,8,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,12,16	4,8	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,12,17	4,8,15,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,12,16,18	4,8,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,12,14	4,8	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,12,14,16,17,18	4,8,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,12,14,18	4,8,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,12,14,16,17	4,8,15,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,12,17	4,8,13,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,12,16,18	4,8,13,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,12,17,18	4,8,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,12,16	4,8,13,15	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,12,14,18	4,8,13,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,12,14,16,17	4,8,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,12,14	4,8,13,15	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,12,14,16,17,18	4,8,13,15,17,18	$2^{-17.5}$

Table 0.1418 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,18	4,8,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,16,17	4,8,11,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3	4,8,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,16,17,18	4,8,11,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,14,17	4,8,11,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,14,16,18	4,8,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,14,17,18	4,8,11,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,14,16	4,8,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3	4,8,11,13	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,16,17,18	4,8,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,18	4,8,11,13,15,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,16,17	4,8,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,14,17,18	4,8,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,14,16	4,8,11,13	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,14,17	4,8,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,14,16,18	4,8,11,13,15,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,12,17	4,8,11,17	2^{-34}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,12,16,18	4,8,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,12,17,18	4,8,11,15,17,18	2^{-34}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,12,16	4,8,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,12,14,18	4,8,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,12,14,16,17	4,8,11,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,12,14	4,8,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,12,14,16,17,18	4,8,11,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,12,17,18	4,8,11,13,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,12,16	4,8,11,13	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,12,17	4,8,11,13,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,12,16,18	4,8,11,13,15,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,12,14	4,8,11,13	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,12,14,16,17,18	4,8,11,13,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,12,14,18	4,8,11,13,15,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,12,14,16,17	4,8,11,13,15,17	$2^{-28.5}$

Table 0.1419 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,10,17,18	4,8,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,10,16	4,8	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,10,17	4,8,15,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,10,16,18	4,8,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,10,14	4,8	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,10,14,16,17,18	4,8,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,10,14,18	4,8,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,10,14,16,17	4,8,15,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,10,17	4,8,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,10,16,18	4,8,13,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,10,17,18	4,8,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,10,16	4,8,13,15	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,10,14,18	4,8,13,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,10,14,16,17	4,8,13,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,10,14	4,8,13,15	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,10,14,16,17,18	4,8,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,10,12	4,8	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,10,12,16,17,18	4,8,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,10,12,18	4,8,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,10,12,16,17	4,8,15,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,10,12,14,17,18	4,8,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,10,12,14,16	4,8	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,10,12,14,17	4,8,15,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,10,12,14,16,18	4,8,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,10,12,18	4,8,13,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,10,12,16,17	4,8,13,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,10,12	4,8,13,15	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,10,12,16,17,18	4,8,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,10,12,14,17	4,8,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,10,12,14,16,18	4,8,13,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,10,12,14,17,18	4,8,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,10,12,14,16	4,8,13,15	2^{-23}

Table 0.1420 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,10,17	4,8,11,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,10,16,18	4,8,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,10,17,18	4,8,11,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,10,16	4,8,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,10,14,18	4,8,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,10,14,16,17	4,8,11,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,10,14	4,8,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,10,14,16,17,18	4,8,11,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,10,17,18	4,8,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,10,16	4,8,11,13	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,10,17	4,8,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,10,16,18	4,8,11,13,15,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,10,14	4,8,11,13	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,10,14,16,17,18	4,8,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,10,14,18	4,8,11,13,15,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,10,14,16,17	4,8,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,10,12,18	4,8,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,10,12,16,17	4,8,11,17	2^{-1}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,10,12	4,8,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,10,12,16,17,18	4,8,11,15,17,18	2^{-1}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,10,12,14,17	4,8,11,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,10,12,14,16,18	4,8,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,10,12,14,17,18	4,8,11,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,10,12,14,16	4,8,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,10,12	4,8,11,13	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,10,12,16,17,18	4,8,11,13,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,10,12,18	4,8,11,13,15,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,10,12,16,17	4,8,11,13,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,10,12,14,17,18	4,8,11,13,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,10,12,14,16	4,8,11,13	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,10,12,14,17	4,8,11,13,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,10,12,14,16,18	4,8,11,13,15,18	2^{-12}

Table 0.1421 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,18	4,8,9,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,16,17	4,8,9,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3	4,8,9,15	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,16,17,18	4,8,9,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,14,17	4,8,9,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,14,16,18	4,8,9,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,14,17,18	4,8,9,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,14,16	4,8,9,15	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3	4,8,9,13	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,16,17,18	4,8,9,13,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,18	4,8,9,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,16,17	4,8,9,13,15,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,14,17,18	4,8,9,13,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,14,16	4,8,9,13	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,14,17	4,8,9,13,15,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,14,16,18	4,8,9,13,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,12,17	4,8,9,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,12,16,18	4,8,9,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,12,17,18	4,8,9,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,12,16	4,8,9,15	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,12,14,18	4,8,9,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,12,14,16,17	4,8,9,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,12,14	4,8,9,15	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,12,14,16,17,18	4,8,9,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,12,17,18	4,8,9,13,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,12,16	4,8,9,13	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,12,17	4,8,9,13,15,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,12,16,18	4,8,9,13,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,12,14	4,8,9,13	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,12,14,16,17,18	4,8,9,13,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,12,14,18	4,8,9,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,12,14,16,17	4,8,9,13,15,17	2^{-23}

Table 0.1422 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3	4,8,9,11	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,16,17,18	4,8,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,18	4,8,9,11,15,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,16,17	4,8,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,14,17,18	4,8,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,14,16	4,8,9,11	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,14,17	4,8,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,14,16,18	4,8,9,11,15,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,18	4,8,9,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,16,17	4,8,9,11,13,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3	4,8,9,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,16,17,18	4,8,9,11,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,14,17	4,8,9,11,13,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,14,16,18	4,8,9,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,14,17,18	4,8,9,11,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,14,16	4,8,9,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,12,17,18	4,8,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,12,16	4,8,9,11	2^{-1}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,12,17	4,8,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,12,16,18	4,8,9,11,15,18	2^{-1}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,12,14	4,8,9,11	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,12,14,16,17,18	4,8,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,12,14,18	4,8,9,11,15,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,12,14,16,17	4,8,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,12,17	4,8,9,11,13,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,12,16,18	4,8,9,11,13,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,12,17,18	4,8,9,11,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,12,16	4,8,9,11,13,15	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,12,14,18	4,8,9,11,13,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,12,14,16,17	4,8,9,11,13,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,12,14	4,8,9,11,13,15	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,12,14,16,17,18	4,8,9,11,13,15,17,18	2^{-12}

Table 0.1423 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,10,17	4,8,9,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,10,16,18	4,8,9,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,10,17,18	4,8,9,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,10,16	4,8,9,15	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,10,14,18	4,8,9,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,10,14,16,17	4,8,9,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,10,14	4,8,9,15	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,10,14,16,17,18	4,8,9,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,10,17,18	4,8,9,13,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,10,16	4,8,9,13	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,10,17	4,8,9,13,15,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,10,16,18	4,8,9,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,10,14	4,8,9,13	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,10,14,16,17,18	4,8,9,13,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,10,14,18	4,8,9,13,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,10,14,16,17	4,8,9,13,15,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,10,12,18	4,8,9,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,10,12,16,17	4,8,9,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,10,12	4,8,9,15	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,10,12,16,17,18	4,8,9,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,10,12,14,17	4,8,9,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,10,12,14,16,18	4,8,9,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,10,12,14,17,18	4,8,9,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,10,12,14,16	4,8,9,15	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,10,12	4,8,9,13	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,10,12,16,17,18	4,8,9,13,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,10,12,18	4,8,9,13,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,10,12,16,17	4,8,9,13,15,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,10,12,14,17,18	4,8,9,13,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,10,12,14,16	4,8,9,13	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,10,12,14,17	4,8,9,13,15,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,10,12,14,16,18	4,8,9,13,15,18	$2^{-17.5}$

Table 0.1424 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,10,17,18	4,8,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,10,16	4,8,9,11	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,10,17	4,8,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,10,16,18	4,8,9,11,15,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,10,14	4,8,9,11	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,10,14,16,17,18	4,8,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,10,14,18	4,8,9,11,15,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,10,14,16,17	4,8,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,10,17	4,8,9,11,13,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,10,16,18	4,8,9,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,10,17,18	4,8,9,11,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,10,16	4,8,9,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,10,14,18	4,8,9,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,10,14,16,17	4,8,9,11,13,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,10,14	4,8,9,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,10,14,16,17,18	4,8,9,11,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,10,12	4,8,9,11	2^{-34}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,10,12,16,17,18	4,8,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,10,12,18	4,8,9,11,15,18	2^{-34}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,10,12,16,17	4,8,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,10,12,14,17,18	4,8,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,10,12,14,16	4,8,9,11	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,10,12,14,17	4,8,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,10,12,14,16,18	4,8,9,11,15,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,10,12,18	4,8,9,11,13,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,10,12,16,17	4,8,9,11,13,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,10,12	4,8,9,11,13,15	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,10,12,16,17,18	4,8,9,11,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,10,12,14,17	4,8,9,11,13,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,10,12,14,16,18	4,8,9,11,13,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,10,12,14,17,18	4,8,9,11,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,10,12,14,16	4,8,9,11,13,15	$2^{-28.5}$

Table 0.1425 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,7,17	4,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,7,16,18	4,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,7,17,18	4,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,7,16	4,15	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,7,14,18	4,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,7,14,16,17	4,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,7,14	4,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,7,14,16,17,18	4,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,7,17,18	4,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,7,16	4,13	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,7,17	4,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,7,16,18	4,13,15,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,7,14	4,13	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,7,14,16,17,18	4,13,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,7,14,18	4,13,15,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,7,14,16,17	4,13,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,7,12,18	4,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,7,12,16,17	4,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,7,12	4,15	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,7,12,16,17,18	4,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,7,12,14,17	4,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,7,12,14,16,18	4,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,7,12,14,17,18	4,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,7,12,14,16	4,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,7,12	4,13	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,7,12,16,17,18	4,13,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,7,12,18	4,13,15,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,7,12,16,17	4,13,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,7,12,14,17,18	4,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,7,12,14,16	4,13	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,7,12,14,17	4,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,7,12,14,16,18	4,13,15,18	2^{-12}

Table 0.1426 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,7,17,18	4,11,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,7,16	4,11	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,7,17	4,11,15,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,7,16,18	4,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,7,14	4,11	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,7,14,16,17,18	4,11,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,7,14,18	4,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,7,14,16,17	4,11,15,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,7,17	4,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,7,16,18	4,11,13,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,7,17,18	4,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,7,16	4,11,13,15	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,7,14,18	4,11,13,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,7,14,16,17	4,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,7,14	4,11,13,15	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,7,14,16,17,18	4,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,7,12	4,11	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,7,12,16,17,18	4,11,17,18	2^{-34}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,7,12,18	4,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,7,12,16,17	4,11,15,17	2^{-34}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,7,12,14,17,18	4,11,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,7,12,14,16	4,11	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,7,12,14,17	4,11,15,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,7,12,14,16,18	4,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,7,12,18	4,11,13,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,7,12,16,17	4,11,13,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,7,12	4,11,13,15	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,7,12,16,17,18	4,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,7,12,14,17	4,11,13,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,7,12,14,16,18	4,11,13,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,7,12,14,17,18	4,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,7,12,14,16	4,11,13,15	2^{-23}

Table 0.1427 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,7,10,18	4,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,7,10,16,17	4,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,7,10	4,15	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,7,10,16,17,18	4,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,7,10,14,17	4,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,7,10,14,16,18	4,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,7,10,14,17,18	4,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,7,10,14,16	4,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,7,10	4,13	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,7,10,16,17,18	4,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,7,10,18	4,13,15,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,7,10,16,17	4,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,7,10,14,17,18	4,13,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,7,10,14,16	4,13	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,7,10,14,17	4,13,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,7,10,14,16,18	4,13,15,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,7,10,12,17	4,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,7,10,12,16,18	4,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,7,10,12,17,18	4,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,7,10,12,16	4,15	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,7,10,12,14,18	4,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,7,10,12,14,16,17	4,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,7,10,12,14	4,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,7,10,12,14,16,17,18	4,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,7,10,12,17,18	4,13,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,7,10,12,16	4,13	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,7,10,12,17	4,13,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,7,10,12,16,18	4,13,15,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,7,10,12,14	4,13	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,7,10,12,14,16,17,18	4,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,7,10,12,14,18	4,13,15,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,7,10,12,14,16,17	4,13,15,17	$2^{-17.5}$

Table 0.1428 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,7,10	4,11	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,7,10,16,17,18	4,11,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,7,10,18	4,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,7,10,16,17	4,11,15,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,7,10,14,17,18	4,11,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,7,10,14,16	4,11	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,7,10,14,17	4,11,15,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,7,10,14,16,18	4,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,7,10,18	4,11,13,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,7,10,16,17	4,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,7,10	4,11,13,15	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,7,10,16,17,18	4,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,7,10,14,17	4,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,7,10,14,16,18	4,11,13,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,7,10,14,17,18	4,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,7,10,14,16	4,11,13,15	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,7,10,12,17,18	4,11,17,18	2^{-1}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,7,10,12,16	4,11	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,7,10,12,17	4,11,15,17	2^{-1}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,7,10,12,16,18	4,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,7,10,12,14	4,11	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,7,10,12,14,16,17,18	4,11,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,7,10,12,14,18	4,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,7,10,12,14,16,17	4,11,15,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,7,10,12,17	4,11,13,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,7,10,12,16,18	4,11,13,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,7,10,12,17,18	4,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,7,10,12,16	4,11,13,15	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,7,10,12,14,18	4,11,13,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,7,10,12,14,16,17	4,11,13,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,7,10,12,14	4,11,13,15	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,7,10,12,14,16,17,18	4,11,13,15,17,18	$2^{-6.5}$

Table 0.1429 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,7,17,18	4,9,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,7,16	4,9	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,7,17	4,9,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,7,16,18	4,9,15,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,7,14	4,9	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,7,14,16,17,18	4,9,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,7,14,18	4,9,15,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,7,14,16,17	4,9,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,7,17	4,9,13,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,7,16,18	4,9,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,7,17,18	4,9,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,7,16	4,9,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,7,14,18	4,9,13,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,7,14,16,17	4,9,13,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,7,14	4,9,13,15	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,7,14,16,17,18	4,9,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,7,12	4,9	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,7,12,16,17,18	4,9,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,7,12,18	4,9,15,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,7,12,16,17	4,9,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,7,12,14,17,18	4,9,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,7,12,14,16	4,9	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,7,12,14,17	4,9,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,7,12,14,16,18	4,9,15,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,7,12,18	4,9,13,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,7,12,16,17	4,9,13,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,7,12	4,9,13,15	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,7,12,16,17,18	4,9,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,7,12,14,17	4,9,13,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,7,12,14,16,18	4,9,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,7,12,14,17,18	4,9,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,7,12,14,16	4,9,13,15	$2^{-17.5}$

Table 0.1430 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,7,17	4,9,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,7,16,18	4,9,11,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,7,17,18	4,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,7,16	4,9,11,15	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,7,14,18	4,9,11,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,7,14,16,17	4,9,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,7,14	4,9,11,15	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,7,14,16,17,18	4,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,7,17,18	4,9,11,13,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,7,16	4,9,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,7,17	4,9,11,13,15,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,7,16,18	4,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,7,14	4,9,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,7,14,16,17,18	4,9,11,13,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,7,14,18	4,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,7,14,16,17	4,9,11,13,15,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,7,12,18	4,9,11,18	2^{-1}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,7,12,16,17	4,9,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,7,12	4,9,11,15	2^{-1}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,7,12,16,17,18	4,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,7,12,14,17	4,9,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,7,12,14,16,18	4,9,11,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,7,12,14,17,18	4,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,7,12,14,16	4,9,11,15	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,7,12	4,9,11,13	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,7,12,16,17,18	4,9,11,13,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,7,12,18	4,9,11,13,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,7,12,16,17	4,9,11,13,15,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,7,12,14,17,18	4,9,11,13,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,7,12,14,16	4,9,11,13	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,7,12,14,17	4,9,11,13,15,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,7,12,14,16,18	4,9,11,13,15,18	$2^{-6.5}$

Table 0.1431 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,7,10	4,9	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,7,10,16,17,18	4,9,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,7,10,18	4,9,15,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,7,10,16,17	4,9,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,7,10,14,17,18	4,9,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,7,10,14,16	4,9	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,7,10,14,17	4,9,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,7,10,14,16,18	4,9,15,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,7,10,18	4,9,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,7,10,16,17	4,9,13,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,7,10	4,9,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,7,10,16,17,18	4,9,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,10,14,17	4,9,13,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,7,10,14,16,18	4,9,13,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,10,14,17,18	4,9,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,7,10,14,16	4,9,13,15	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,7,10,12,17,18	4,9,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,7,10,12,16	4,9	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,7,10,12,17	4,9,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,7,10,12,16,18	4,9,15,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,7,10,12,14	4,9	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,7,10,12,14,16,17,18	4,9,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,7,10,12,14,18	4,9,15,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,7,10,12,14,16,17	4,9,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,7,10,12,17	4,9,13,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,7,10,12,16,18	4,9,13,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,7,10,12,17,18	4,9,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,7,10,12,16	4,9,13,15	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,7,10,12,14,18	4,9,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,7,10,12,14,16,17	4,9,13,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,7,10,12,14	4,9,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,7,10,12,14,16,17,18	4,9,13,15,17,18	2^{-12}

Table 0.1432 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,7,10,18	4,9,11,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,7,10,16,17	4,9,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,7,10	4,9,11,15	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,7,10,16,17,18	4,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,7,10,14,17	4,9,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,7,10,14,16,18	4,9,11,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,7,10,14,17,18	4,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,7,10,14,16	4,9,11,15	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,7,10	4,9,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,7,10,16,17,18	4,9,11,13,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,7,10,18	4,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,7,10,16,17	4,9,11,13,15,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,7,10,14,17,18	4,9,11,13,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,7,10,14,16	4,9,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,7,10,14,17	4,9,11,13,15,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,7,10,14,16,18	4,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,7,10,12,17	4,9,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,7,10,12,16,18	4,9,11,18	2^{-34}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,7,10,12,17,18	4,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,7,10,12,16	4,9,11,15	2^{-34}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,7,10,12,14,18	4,9,11,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,7,10,12,14,16,17	4,9,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,7,10,12,14	4,9,11,15	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,7,10,12,14,16,17,18	4,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,7,10,12,17,18	4,9,11,13,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,7,10,12,16	4,9,11,13	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,7,10,12,17	4,9,11,13,15,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,7,10,12,16,18	4,9,11,13,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,7,10,12,14	4,9,11,13	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,7,10,12,14,16,17,18	4,9,11,13,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,7,10,12,14,18	4,9,11,13,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,7,10,12,14,16,17	4,9,11,13,15,17	2^{-23}

Table 0.1433 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,7,18	4,8,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,7,16,17	4,8,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,7	4,8,15	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,7,16,17,18	4,8,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,7,14,17	4,8,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,7,14,16,18	4,8,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,7,14,17,18	4,8,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,7,14,16	4,8,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,7	4,8,13	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,7,16,17,18	4,8,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,7,18	4,8,13,15,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,7,16,17	4,8,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,7,14,17,18	4,8,13,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,14,16	4,8,13	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,7,14,17	4,8,13,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,14,16,18	4,8,13,15,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,7,12,17	4,8,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,7,12,16,18	4,8,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,7,12,17,18	4,8,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,7,12,16	4,8,15	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,7,12,14,18	4,8,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,7,12,14,16,17	4,8,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,7,12,14	4,8,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,7,12,14,16,17,18	4,8,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,7,12,17,18	4,8,13,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,7,12,16	4,8,13	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,7,12,17	4,8,13,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,7,12,16,18	4,8,13,15,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,7,12,14	4,8,13	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,7,12,14,16,17,18	4,8,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,7,12,14,18	4,8,13,15,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,7,12,14,16,17	4,8,13,15,17	$2^{-17.5}$

Table 0.1434 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,7	4,8,11	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,7,16,17,18	4,8,11,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,7,18	4,8,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,7,16,17	4,8,11,15,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,7,14,17,18	4,8,11,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,7,14,16	4,8,11	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,7,14,17	4,8,11,15,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,7,14,16,18	4,8,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,7,18	4,8,11,13,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,7,16,17	4,8,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,7	4,8,11,13,15	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,7,16,17,18	4,8,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,7,14,17	4,8,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,7,14,16,18	4,8,11,13,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,7,14,17,18	4,8,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,7,14,16	4,8,11,13,15	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,7,12,17,18	4,8,11,17,18	2^{-34}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,7,12,16	4,8,11	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,7,12,17	4,8,11,15,17	2^{-34}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,7,12,16,18	4,8,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,7,12,14	4,8,11	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,7,12,14,16,17,18	4,8,11,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,7,12,14,18	4,8,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,7,12,14,16,17	4,8,11,15,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,7,12,17	4,8,11,13,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,7,12,16,18	4,8,11,13,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,7,12,17,18	4,8,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,7,12,16	4,8,11,13,15	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,7,12,14,18	4,8,11,13,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,7,12,14,16,17	4,8,11,13,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,7,12,14	4,8,11,13,15	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,7,12,14,16,17,18	4,8,11,13,15,17,18	$2^{-28.5}$

Table 0.1435 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,7,10,17	4,8,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,7,10,16,18	4,8,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,7,10,17,18	4,8,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,7,10,16	4,8,15	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,7,10,14,18	4,8,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,7,10,14,16,17	4,8,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,7,10,14	4,8,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,7,10,14,16,17,18	4,8,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,7,10,17,18	4,8,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,7,10,16	4,8,13	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,7,10,17	4,8,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,7,10,16,18	4,8,13,15,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,7,10,14	4,8,13	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,7,10,14,16,17,18	4,8,13,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,7,10,14,18	4,8,13,15,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,7,10,14,16,17	4,8,13,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,7,10,12,18	4,8,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,7,10,12,16,17	4,8,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,7,10,12	4,8,15	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,7,10,12,16,17,18	4,8,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,7,10,12,14,17	4,8,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,7,10,12,14,16,18	4,8,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,7,10,12,14,17,18	4,8,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,7,10,12,14,16	4,8,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,7,10,12	4,8,13	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,7,10,12,16,17,18	4,8,13,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,7,10,12,18	4,8,13,15,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,7,10,12,16,17	4,8,13,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,7,10,12,14,17,18	4,8,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,7,10,12,14,16	4,8,13	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,7,10,12,14,17	4,8,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,7,10,12,14,16,18	4,8,13,15,18	2^{-23}

Table 0.1436 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,7,10,17,18	4,8,11,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,7,10,16	4,8,11	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,7,10,17	4,8,11,15,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,7,10,16,18	4,8,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,7,10,14	4,8,11	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,7,10,14,16,17,18	4,8,11,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,7,10,14,18	4,8,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,7,10,14,16,17	4,8,11,15,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,7,10,17	4,8,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,7,10,16,18	4,8,11,13,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,7,10,17,18	4,8,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,7,10,16	4,8,11,13,15	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,7,10,14,18	4,8,11,13,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,7,10,14,16,17	4,8,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,7,10,14	4,8,11,13,15	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,7,10,14,16,17,18	4,8,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,7,10,12	4,8,11	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,7,10,12,16,17,18	4,8,11,17,18	2^{-1}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,7,10,12,18	4,8,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,7,10,12,16,17	4,8,11,15,17	2^{-1}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,7,10,12,14,17,18	4,8,11,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,7,10,12,14,16	4,8,11	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,7,10,12,14,17	4,8,11,15,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,7,10,12,14,16,18	4,8,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,7,10,12,18	4,8,11,13,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,7,10,12,16,17	4,8,11,13,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,7,10,12	4,8,11,13,15	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,7,10,12,16,17,18	4,8,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,7,10,12,14,17	4,8,11,13,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,7,10,12,14,16,18	4,8,11,13,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,7,10,12,14,17,18	4,8,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,7,10,12,14,16	4,8,11,13,15	2^{-12}

Table 0.1437 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,7	4,8,9	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,7,16,17,18	4,8,9,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,7,18	4,8,9,15,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,7,16,17	4,8,9,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,7,14,17,18	4,8,9,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,7,14,16	4,8,9	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,7,14,17	4,8,9,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,7,14,16,18	4,8,9,15,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,7,18	4,8,9,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,7,16,17	4,8,9,13,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,7	4,8,9,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,7,16,17,18	4,8,9,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,7,14,17	4,8,9,13,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,7,14,16,18	4,8,9,13,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,7,14,17,18	4,8,9,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,7,14,16	4,8,9,13,15	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,7,12,17,18	4,8,9,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,7,12,16	4,8,9	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,7,12,17	4,8,9,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,7,12,16,18	4,8,9,15,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,7,12,14	4,8,9	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,7,12,14,16,17,18	4,8,9,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,7,12,14,18	4,8,9,15,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,7,12,14,16,17	4,8,9,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,7,12,17	4,8,9,13,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,7,12,16,18	4,8,9,13,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,7,12,17,18	4,8,9,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,7,12,16	4,8,9,13,15	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,7,12,14,18	4,8,9,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,7,12,14,16,17	4,8,9,13,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,7,12,14	4,8,9,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,7,12,14,16,17,18	4,8,9,13,15,17,18	2^{-23}

Table 0.1438 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,7,18	4,8,9,11,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,7,16,17	4,8,9,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,7	4,8,9,11,15	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,7,16,17,18	4,8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,7,14,17	4,8,9,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,7,14,16,18	4,8,9,11,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,7,14,17,18	4,8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,7,14,16	4,8,9,11,15	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,7	4,8,9,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,7,16,17,18	4,8,9,11,13,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,7,18	4,8,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,7,16,17	4,8,9,11,13,15,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,7,14,17,18	4,8,9,11,13,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,7,14,16	4,8,9,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,7,14,17	4,8,9,11,13,15,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,7,14,16,18	4,8,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,7,12,17	4,8,9,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,7,12,16,18	4,8,9,11,18	2^{-1}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,7,12,17,18	4,8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,7,12,16	4,8,9,11,15	2^{-1}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,7,12,14,18	4,8,9,11,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,7,12,14,16,17	4,8,9,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,7,12,14	4,8,9,11,15	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,7,12,14,16,17,18	4,8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,7,12,17,18	4,8,9,11,13,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,7,12,16	4,8,9,11,13	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,7,12,17	4,8,9,11,13,15,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,7,12,16,18	4,8,9,11,13,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,7,12,14	4,8,9,11,13	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,7,12,14,16,17,18	4,8,9,11,13,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,7,12,14,18	4,8,9,11,13,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,7,12,14,16,17	4,8,9,11,13,15,17	2^{-12}

Table 0.1439 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,7,10,17,18	4,8,9,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,7,10,16	4,8,9	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,7,10,17	4,8,9,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,7,10,16,18	4,8,9,15,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,7,10,14	4,8,9	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,7,10,14,16,17,18	4,8,9,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,7,10,14,18	4,8,9,15,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,7,10,14,16,17	4,8,9,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,7,10,17	4,8,9,13,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,7,10,16,18	4,8,9,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,7,10,17,18	4,8,9,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,7,10,16	4,8,9,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,7,10,14,18	4,8,9,13,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,7,10,14,16,17	4,8,9,13,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,7,10,14	4,8,9,13,15	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,7,10,14,16,17,18	4,8,9,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,7,10,12	4,8,9	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,7,10,12,16,17,18	4,8,9,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,7,10,12,18	4,8,9,15,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,7,10,12,16,17	4,8,9,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,7,10,12,14,17,18	4,8,9,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,7,10,12,14,16	4,8,9	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,7,10,12,14,17	4,8,9,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,7,10,12,14,16,18	4,8,9,15,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,7,10,12,18	4,8,9,13,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,7,10,12,16,17	4,8,9,13,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,7,10,12	4,8,9,13,15	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,7,10,12,16,17,18	4,8,9,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,7,10,12,14,17	4,8,9,13,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,7,10,12,14,16,18	4,8,9,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,7,10,12,14,17,18	4,8,9,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,7,10,12,14,16	4,8,9,13,15	$2^{-17.5}$

Table 0.1440 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,7,10,17	4,8,9,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,7,10,16,18	4,8,9,11,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,7,10,17,18	4,8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,7,10,16	4,8,9,11,15	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,7,10,14,18	4,8,9,11,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,7,10,14,16,17	4,8,9,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,7,10,14	4,8,9,11,15	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,7,10,14,16,17,18	4,8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,7,10,17,18	4,8,9,11,13,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,7,10,16	4,8,9,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,7,10,17	4,8,9,11,13,15,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,7,10,16,18	4,8,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,7,10,14	4,8,9,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,7,10,14,16,17,18	4,8,9,11,13,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,7,10,14,18	4,8,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,7,10,14,16,17	4,8,9,11,13,15,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,7,10,12,18	4,8,9,11,18	2^{-34}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,7,10,12,16,17	4,8,9,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,7,10,12	4,8,9,11,15	2^{-34}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,7,10,12,16,17,18	4,8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,7,10,12,14,17	4,8,9,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,7,10,12,14,16,18	4,8,9,11,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,7,10,12,14,17,18	4,8,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,7,10,12,14,16	4,8,9,11,15	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,7,10,12	4,8,9,11,13	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,7,10,12,16,17,18	4,8,9,11,13,17,18	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,7,10,12,18	4,8,9,11,13,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,7,10,12,16,17	4,8,9,11,13,15,17	2^{-12}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,7,10,12,14,17,18	4,8,9,11,13,17,18	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,7,10,12,14,16	4,8,9,11,13	$2^{-28.5}$
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,7,10,12,14,17	4,8,9,11,13,15,17	2^{-23}
$(1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,7,10,12,14,16,18	4,8,9,11,13,15,18	$2^{-28.5}$

Table 0.1441 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3	4,6	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,16,17,18	4,6,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,18	4,6,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,16,17	4,6,15,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,14,17,18	4,6,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,14,16	4,6	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,14,17	4,6,15,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,14,16,18	4,6,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,18	4,6,13,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,16,17	4,6,13,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3	4,6,13,15	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,16,17,18	4,6,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,14,17	4,6,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,14,16,18	4,6,13,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,14,17,18	4,6,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,14,16	4,6,13,15	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,12,17,18	4,6,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,12,16	4,6	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,12,17	4,6,15,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,12,16,18	4,6,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,12,14	4,6	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,12,14,16,17,18	4,6,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,12,14,18	4,6,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,12,14,16,17	4,6,15,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,12,17	4,6,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,12,16,18	4,6,13,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,12,17,18	4,6,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,12,16	4,6,13,15	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,12,14,18	4,6,13,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,12,14,16,17	4,6,13,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,12,14	4,6,13,15	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,12,14,16,17,18	4,6,13,15,17,18	$2^{-28.5}$

Table 0.1442 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,18	4,6,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,16,17	4,6,11,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3	4,6,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,16,17,18	4,6,11,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,14,17	4,6,11,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,14,16,18	4,6,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,14,17,18	4,6,11,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,14,16	4,6,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3	4,6,11,13	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,16,17,18	4,6,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,18	4,6,11,13,15,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,16,17	4,6,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,14,17,18	4,6,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,14,16	4,6,11,13	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,14,17	4,6,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,14,16,18	4,6,11,13,15,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,12,17	4,6,11,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,12,16,18	4,6,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,12,17,18	4,6,11,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,12,16	4,6,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,12,14,18	4,6,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,12,14,16,17	4,6,11,17	2^{-34}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,12,14	4,6,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,12,14,16,17,18	4,6,11,15,17,18	2^{-34}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,12,17,18	4,6,11,13,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,12,16	4,6,11,13	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,12,17	4,6,11,13,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,12,16,18	4,6,11,13,15,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,12,14	4,6,11,13	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,12,14,16,17,18	4,6,11,13,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,12,14,18	4,6,11,13,15,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,12,14,16,17	4,6,11,13,15,17	$2^{-28.5}$

Table 0.1443 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,10,17,18	4,6,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,10,16	4,6	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,10,17	4,6,15,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,10,16,18	4,6,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,10,14	4,6	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,10,14,16,17,18	4,6,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,10,14,18	4,6,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,10,14,16,17	4,6,15,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,10,17	4,6,13,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,10,16,18	4,6,13,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,10,17,18	4,6,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,10,16	4,6,13,15	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,10,14,18	4,6,13,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,10,14,16,17	4,6,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,10,14	4,6,13,15	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,10,14,16,17,18	4,6,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,10,12	4,6	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,10,12,16,17,18	4,6,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,10,12,18	4,6,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,10,12,16,17	4,6,15,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,10,12,14,17,18	4,6,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,10,12,14,16	4,6	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,10,12,14,17	4,6,15,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,10,12,14,16,18	4,6,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,10,12,18	4,6,13,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,10,12,16,17	4,6,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,10,12	4,6,13,15	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,10,12,16,17,18	4,6,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,10,12,14,17	4,6,13,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,10,12,14,16,18	4,6,13,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,10,12,14,17,18	4,6,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,10,12,14,16	4,6,13,15	2^{-23}

Table 0.1444 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,10,17	4,6,11,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,10,16,18	4,6,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,10,17,18	4,6,11,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,10,16	4,6,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,10,14,18	4,6,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,10,14,16,17	4,6,11,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,10,14	4,6,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,10,14,16,17,18	4,6,11,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,10,17,18	4,6,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,10,16	4,6,11,13	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,10,17	4,6,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,10,16,18	4,6,11,13,15,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,10,14	4,6,11,13	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,10,14,16,17,18	4,6,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,10,14,18	4,6,11,13,15,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,10,14,16,17	4,6,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,10,12,18	4,6,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,10,12,16,17	4,6,11,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,10,12	4,6,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,10,12,16,17,18	4,6,11,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,10,12,14,17	4,6,11,17	2^{-1}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,10,12,14,16,18	4,6,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,10,12,14,17,18	4,6,11,15,17,18	2^{-1}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,10,12,14,16	4,6,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,10,12	4,6,11,13	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,10,12,16,17,18	4,6,11,13,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,10,12,18	4,6,11,13,15,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,10,12,16,17	4,6,11,13,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,10,12,14,17,18	4,6,11,13,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,10,12,14,16	4,6,11,13	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,10,12,14,17	4,6,11,13,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,10,12,14,16,18	4,6,11,13,15,18	2^{-23}

Table 0.1445 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,18	4,6,9,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,16,17	4,6,9,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3	4,6,9,15	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,16,17,18	4,6,9,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,14,17	4,6,9,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,14,16,18	4,6,9,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,14,17,18	4,6,9,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,14,16	4,6,9,15	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3	4,6,9,13	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,16,17,18	4,6,9,13,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,18	4,6,9,13,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,16,17	4,6,9,13,15,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,14,17,18	4,6,9,13,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,14,16	4,6,9,13	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,14,17	4,6,9,13,15,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,14,16,18	4,6,9,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,12,17	4,6,9,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,12,16,18	4,6,9,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,12,17,18	4,6,9,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,12,16	4,6,9,15	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,12,14,18	4,6,9,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,12,14,16,17	4,6,9,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,12,14	4,6,9,15	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,12,14,16,17,18	4,6,9,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,12,17,18	4,6,9,13,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,12,16	4,6,9,13	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,12,17	4,6,9,13,15,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,12,16,18	4,6,9,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,12,14	4,6,9,13	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,12,14,16,17,18	4,6,9,13,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,12,14,18	4,6,9,13,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,12,14,16,17	4,6,9,13,15,17	2^{-23}

Table 0.1446 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3	4,6,9,11	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,16,17,18	4,6,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,18	4,6,9,11,15,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,16,17	4,6,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,14,17,18	4,6,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,14,16	4,6,9,11	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,14,17	4,6,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,14,16,18	4,6,9,11,15,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,18	4,6,9,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,16,17	4,6,9,11,13,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3	4,6,9,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,16,17,18	4,6,9,11,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,14,17	4,6,9,11,13,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,14,16,18	4,6,9,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,14,17,18	4,6,9,11,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,14,16	4,6,9,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,12,17,18	4,6,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,12,16	4,6,9,11	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,12,17	4,6,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,12,16,18	4,6,9,11,15,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,12,14	4,6,9,11	2^{-1}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,12,14,16,17,18	4,6,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,12,14,18	4,6,9,11,15,18	2^{-1}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,12,14,16,17	4,6,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,12,17	4,6,9,11,13,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,12,16,18	4,6,9,11,13,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,12,17,18	4,6,9,11,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,12,16	4,6,9,11,13,15	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,12,14,18	4,6,9,11,13,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,12,14,16,17	4,6,9,11,13,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,12,14	4,6,9,11,13,15	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,12,14,16,17,18	4,6,9,11,13,15,17,18	2^{-23}

Table 0.1447 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,10,17	4,6,9,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,10,16,18	4,6,9,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,10,17,18	4,6,9,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,10,16	4,6,9,15	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,10,14,18	4,6,9,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,10,14,16,17	4,6,9,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,10,14	4,6,9,15	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,10,14,16,17,18	4,6,9,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,10,17,18	4,6,9,13,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,10,16	4,6,9,13	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,10,17	4,6,9,13,15,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,10,16,18	4,6,9,13,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,10,14	4,6,9,13	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,10,14,16,17,18	4,6,9,13,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,10,14,18	4,6,9,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,10,14,16,17	4,6,9,13,15,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,10,12,18	4,6,9,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,10,12,16,17	4,6,9,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,10,12	4,6,9,15	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,10,12,16,17,18	4,6,9,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,10,12,14,17	4,6,9,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,10,12,14,16,18	4,6,9,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,10,12,14,17,18	4,6,9,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,10,12,14,16	4,6,9,15	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,10,12	4,6,9,13	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,10,12,16,17,18	4,6,9,13,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,10,12,18	4,6,9,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,10,12,16,17	4,6,9,13,15,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,10,12,14,17,18	4,6,9,13,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,10,12,14,16	4,6,9,13	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,10,12,14,17	4,6,9,13,15,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,10,12,14,16,18	4,6,9,13,15,18	$2^{-28.5}$

Table 0.1448 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,10,17,18	4,6,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,10,16	4,6,9,11	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,10,17	4,6,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,10,16,18	4,6,9,11,15,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,10,14	4,6,9,11	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,10,14,16,17,18	4,6,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,10,14,18	4,6,9,11,15,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,10,14,16,17	4,6,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,10,17	4,6,9,11,13,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,10,16,18	4,6,9,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,10,17,18	4,6,9,11,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,10,16	4,6,9,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,10,14,18	4,6,9,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,10,14,16,17	4,6,9,11,13,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,10,14	4,6,9,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,10,14,16,17,18	4,6,9,11,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,10,12	4,6,9,11	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,10,12,16,17,18	4,6,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,10,12,18	4,6,9,11,15,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,10,12,16,17	4,6,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,10,12,14,17,18	4,6,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,10,12,14,16	4,6,9,11	2^{-34}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,10,12,14,17	4,6,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,10,12,14,16,18	4,6,9,11,15,18	2^{-34}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,10,12,18	4,6,9,11,13,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,10,12,16,17	4,6,9,11,13,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,10,12	4,6,9,11,13,15	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,10,12,16,17,18	4,6,9,11,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,10,12,14,17	4,6,9,11,13,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,10,12,14,16,18	4,6,9,11,13,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,10,12,14,17,18	4,6,9,11,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,10,12,14,16	4,6,9,11,13,15	$2^{-28.5}$

Table 0.1449 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,17,18	4,6,8,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,16	4,6,8	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,17	4,6,8,15,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,16,18	4,6,8,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,14	4,6,8	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,14,16,17,18	4,6,8,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,14,18	4,6,8,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,14,16,17	4,6,8,15,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,17	4,6,8,13,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,16,18	4,6,8,13,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,17,18	4,6,8,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,16	4,6,8,13,15	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,14,18	4,6,8,13,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,14,16,17	4,6,8,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,14	4,6,8,13,15	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,14,16,17,18	4,6,8,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,12	4,6,8	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,12,16,17,18	4,6,8,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,12,18	4,6,8,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,12,16,17	4,6,8,15,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,12,14,17,18	4,6,8,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,12,14,16	4,6,8	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,12,14,17	4,6,8,15,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,12,14,16,18	4,6,8,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,12,18	4,6,8,13,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,12,16,17	4,6,8,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,12	4,6,8,13,15	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,12,16,17,18	4,6,8,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,12,14,17	4,6,8,13,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,12,14,16,18	4,6,8,13,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,12,14,17,18	4,6,8,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,12,14,16	4,6,8,13,15	2^{-12}

Table 0.1450 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,17	4,6,8,11,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,16,18	4,6,8,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,17,18	4,6,8,11,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,16	4,6,8,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,14,18	4,6,8,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,14,16,17	4,6,8,11,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,14	4,6,8,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,14,16,17,18	4,6,8,11,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,17,18	4,6,8,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,16	4,6,8,11,13	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,17	4,6,8,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,16,18	4,6,8,11,13,15,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,14	4,6,8,11,13	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,14,16,17,18	4,6,8,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,14,18	4,6,8,11,13,15,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,14,16,17	4,6,8,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,12,18	4,6,8,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,12,16,17	4,6,8,11,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,12	4,6,8,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,12,16,17,18	4,6,8,11,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,12,14,17	4,6,8,11,17	2^{-34}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,12,14,16,18	4,6,8,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,12,14,17,18	4,6,8,11,15,17,18	2^{-34}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,12,14,16	4,6,8,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,12	4,6,8,11,13	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,12,16,17,18	4,6,8,11,13,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,12,18	4,6,8,11,13,15,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,12,16,17	4,6,8,11,13,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,12,14,17,18	4,6,8,11,13,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,12,14,16	4,6,8,11,13	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,12,14,17	4,6,8,11,13,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,12,14,16,18	4,6,8,11,13,15,18	2^{-12}

Table 0.1451 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,10	4,6,8	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,10,16,17,18	4,6,8,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,10,18	4,6,8,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,10,16,17	4,6,8,15,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,10,14,17,18	4,6,8,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,10,14,16	4,6,8	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,10,14,17	4,6,8,15,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,10,14,16,18	4,6,8,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,10,18	4,6,8,13,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,10,16,17	4,6,8,13,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,10	4,6,8,13,15	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,10,16,17,18	4,6,8,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,10,14,17	4,6,8,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,10,14,16,18	4,6,8,13,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,10,14,17,18	4,6,8,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,10,14,16	4,6,8,13,15	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,10,12,17,18	4,6,8,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,10,12,16	4,6,8	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,10,12,17	4,6,8,15,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,10,12,16,18	4,6,8,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,10,12,14	4,6,8	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,10,12,14,16,17,18	4,6,8,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,10,12,14,18	4,6,8,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,10,12,14,16,17	4,6,8,15,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,10,12,17	4,6,8,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,10,12,16,18	4,6,8,13,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,10,12,17,18	4,6,8,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,10,12,16	4,6,8,13,15	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,10,12,14,18	4,6,8,13,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,10,12,14,16,17	4,6,8,13,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,10,12,14	4,6,8,13,15	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,10,12,14,16,17,18	4,6,8,13,15,17,18	$2^{-6.5}$

Table 0.1452 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,10,18	4,6,8,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,10,16,17	4,6,8,11,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,10	4,6,8,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,10,16,17,18	4,6,8,11,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,10,14,17	4,6,8,11,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,10,14,16,18	4,6,8,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,10,14,17,18	4,6,8,11,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,10,14,16	4,6,8,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,10	4,6,8,11,13	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,10,16,17,18	4,6,8,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,10,18	4,6,8,11,13,15,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,10,16,17	4,6,8,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,10,14,17,18	4,6,8,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,10,14,16	4,6,8,11,13	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,10,14,17	4,6,8,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,10,14,16,18	4,6,8,11,13,15,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,10,12,17	4,6,8,11,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,10,12,16,18	4,6,8,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,10,12,17,18	4,6,8,11,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,10,12,16	4,6,8,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,10,12,14,18	4,6,8,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,10,12,14,16,17	4,6,8,11,17	2^{-1}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,10,12,14	4,6,8,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,10,12,14,16,17,18	4,6,8,11,15,17,18	2^{-1}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,10,12,17,18	4,6,8,11,13,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,10,12,16	4,6,8,11,13	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,10,12,17	4,6,8,11,13,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,10,12,16,18	4,6,8,11,13,15,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,10,12,14	4,6,8,11,13	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,10,12,14,16,17,18	4,6,8,11,13,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,10,12,14,18	4,6,8,11,13,15,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,10,12,14,16,17	4,6,8,11,13,15,17	$2^{-6.5}$

Table 0.1453 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,17	4,6,8,9,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,16,18	4,6,8,9,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,17,18	4,6,8,9,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,16	4,6,8,9,15	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,14,18	4,6,8,9,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,14,16,17	4,6,8,9,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,14	4,6,8,9,15	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,14,16,17,18	4,6,8,9,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,17,18	4,6,8,9,13,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,16	4,6,8,9,13	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,17	4,6,8,9,13,15,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,16,18	4,6,8,9,13,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,14	4,6,8,9,13	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,14,16,17,18	4,6,8,9,13,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,14,18	4,6,8,9,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,14,16,17	4,6,8,9,13,15,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,12,18	4,6,8,9,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,12,16,17	4,6,8,9,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,12	4,6,8,9,15	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,12,16,17,18	4,6,8,9,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,12,14,17	4,6,8,9,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,12,14,16,18	4,6,8,9,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,12,14,17,18	4,6,8,9,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,12,14,16	4,6,8,9,15	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,12	4,6,8,9,13	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,12,16,17,18	4,6,8,9,13,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,12,18	4,6,8,9,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,12,16,17	4,6,8,9,13,15,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,12,14,17,18	4,6,8,9,13,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,12,14,16	4,6,8,9,13	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,12,14,17	4,6,8,9,13,15,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,12,14,16,18	4,6,8,9,13,15,18	$2^{-6.5}$

Table 0.1454 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,17,18	4,6,8,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,16	4,6,8,9,11	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,17	4,6,8,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,16,18	4,6,8,9,11,15,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,14	4,6,8,9,11	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,14,16,17,18	4,6,8,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,14,18	4,6,8,9,11,15,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,14,16,17	4,6,8,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,17	4,6,8,9,11,13,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,16,18	4,6,8,9,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,17,18	4,6,8,9,11,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,16	4,6,8,9,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,14,18	4,6,8,9,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,14,16,17	4,6,8,9,11,13,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,14	4,6,8,9,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,14,16,17,18	4,6,8,9,11,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,12	4,6,8,9,11	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,12,16,17,18	4,6,8,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,12,18	4,6,8,9,11,15,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,12,16,17	4,6,8,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,12,14,17,18	4,6,8,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,12,14,16	4,6,8,9,11	2^{-1}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,12,14,17	4,6,8,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,12,14,16,18	4,6,8,9,11,15,18	2^{-1}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,12,18	4,6,8,9,11,13,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,12,16,17	4,6,8,9,11,13,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,12	4,6,8,9,11,13,15	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,12,16,17,18	4,6,8,9,11,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,12,14,17	4,6,8,9,11,13,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,12,14,16,18	4,6,8,9,11,13,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,12,14,17,18	4,6,8,9,11,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,12,14,16	4,6,8,9,11,13,15	$2^{-6.5}$

Table 0.1455 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,10,18	4,6,8,9,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,10,16,17	4,6,8,9,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,10	4,6,8,9,15	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,10,16,17,18	4,6,8,9,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,10,14,17	4,6,8,9,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,10,14,16,18	4,6,8,9,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,10,14,17,18	4,6,8,9,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,10,14,16	4,6,8,9,15	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,10	4,6,8,9,13	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,10,16,17,18	4,6,8,9,13,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,10,18	4,6,8,9,13,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,10,16,17	4,6,8,9,13,15,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,10,14,17,18	4,6,8,9,13,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,10,14,16	4,6,8,9,13	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,10,14,17	4,6,8,9,13,15,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,10,14,16,18	4,6,8,9,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,10,12,17	4,6,8,9,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,10,12,16,18	4,6,8,9,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,10,12,17,18	4,6,8,9,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,10,12,16	4,6,8,9,15	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,10,12,14,18	4,6,8,9,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,10,12,14,16,17	4,6,8,9,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,10,12,14	4,6,8,9,15	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,10,12,14,16,17,18	4,6,8,9,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,10,12,17,18	4,6,8,9,13,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,10,12,16	4,6,8,9,13	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,10,12,17	4,6,8,9,13,15,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,10,12,16,18	4,6,8,9,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,10,12,14	4,6,8,9,13	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,10,12,14,16,17,18	4,6,8,9,13,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,10,12,14,18	4,6,8,9,13,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,10,12,14,16,17	4,6,8,9,13,15,17	2^{-12}

Table 0.1456 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,10	4,6,8,9,11	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,10,16,17,18	4,6,8,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,10,18	4,6,8,9,11,15,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,10,16,17	4,6,8,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,10,14,17,18	4,6,8,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,10,14,16	4,6,8,9,11	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,10,14,17	4,6,8,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,10,14,16,18	4,6,8,9,11,15,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,10,18	4,6,8,9,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,10,16,17	4,6,8,9,11,13,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,10	4,6,8,9,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,10,16,17,18	4,6,8,9,11,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,10,14,17	4,6,8,9,11,13,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,10,14,16,18	4,6,8,9,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,10,14,17,18	4,6,8,9,11,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,10,14,16	4,6,8,9,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,10,12,17,18	4,6,8,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,10,12,16	4,6,8,9,11	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,10,12,17	4,6,8,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,10,12,16,18	4,6,8,9,11,15,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,10,12,14	4,6,8,9,11	2^{-34}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,10,12,14,16,17,18	4,6,8,9,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,10,12,14,18	4,6,8,9,11,15,18	2^{-34}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,10,12,14,16,17	4,6,8,9,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,10,12,17	4,6,8,9,11,13,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,10,12,16,18	4,6,8,9,11,13,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,10,12,17,18	4,6,8,9,11,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,10,12,16	4,6,8,9,11,13,15	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,10,12,14,18	4,6,8,9,11,13,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,10,12,14,16,17	4,6,8,9,11,13,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,10,12,14	4,6,8,9,11,13,15	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,10,12,14,16,17,18	4,6,8,9,11,13,15,17,18	2^{-12}

Table 0.1457 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,7,18	4,6,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,7,16,17	4,6,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,7	4,6,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,7,16,17,18	4,6,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,7,14,17	4,6,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,7,14,16,18	4,6,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,7,14,17,18	4,6,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,7,14,16	4,6,15	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,7	4,6,13	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,7,16,17,18	4,6,13,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,7,18	4,6,13,15,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,7,16,17	4,6,13,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,7,14,17,18	4,6,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,7,14,16	4,6,13	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,7,14,17	4,6,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,7,14,16,18	4,6,13,15,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,7,12,17	4,6,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,7,12,16,18	4,6,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,7,12,17,18	4,6,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,7,12,16	4,6,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,7,12,14,18	4,6,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,7,12,14,16,17	4,6,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,7,12,14	4,6,15	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,7,12,14,16,17,18	4,6,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,7,12,17,18	4,6,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,7,12,16	4,6,13	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,7,12,17	4,6,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,7,12,16,18	4,6,13,15,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,7,12,14	4,6,13	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,7,12,14,16,17,18	4,6,13,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,7,12,14,18	4,6,13,15,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,7,12,14,16,17	4,6,13,15,17	$2^{-28.5}$

Table 0.1458 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,7	4,6,11	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,7,16,17,18	4,6,11,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,7,18	4,6,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,7,16,17	4,6,11,15,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,7,14,17,18	4,6,11,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,7,14,16	4,6,11	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,7,14,17	4,6,11,15,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,7,14,16,18	4,6,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,7,18	4,6,11,13,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,7,16,17	4,6,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,7	4,6,11,13,15	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,7,16,17,18	4,6,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,7,14,17	4,6,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,7,14,16,18	4,6,11,13,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,7,14,17,18	4,6,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,7,14,16	4,6,11,13,15	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,7,12,17,18	4,6,11,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,7,12,16	4,6,11	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,7,12,17	4,6,11,15,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,7,12,16,18	4,6,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,7,12,14	4,6,11	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,7,12,14,16,17,18	4,6,11,17,18	2^{-34}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,7,12,14,18	4,6,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,7,12,14,16,17	4,6,11,15,17	2^{-34}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,7,12,17	4,6,11,13,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,7,12,16,18	4,6,11,13,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,7,12,17,18	4,6,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,7,12,16	4,6,11,13,15	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,7,12,14,18	4,6,11,13,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,7,12,14,16,17	4,6,11,13,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,7,12,14	4,6,11,13,15	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,7,12,14,16,17,18	4,6,11,13,15,17,18	$2^{-28.5}$

Table 0.1459 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,7,10,17	4,6,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,7,10,16,18	4,6,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,7,10,17,18	4,6,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,7,10,16	4,6,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,7,10,14,18	4,6,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,7,10,14,16,17	4,6,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,7,10,14	4,6,15	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,7,10,14,16,17,18	4,6,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,7,10,17,18	4,6,13,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,7,10,16	4,6,13	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,7,10,17	4,6,13,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,7,10,16,18	4,6,13,15,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,7,10,14	4,6,13	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,7,10,14,16,17,18	4,6,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,7,10,14,18	4,6,13,15,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,7,10,14,16,17	4,6,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,7,10,12,18	4,6,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,7,10,12,16,17	4,6,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,7,10,12	4,6,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,7,10,12,16,17,18	4,6,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,7,10,12,14,17	4,6,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,7,10,12,14,16,18	4,6,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,7,10,12,14,17,18	4,6,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,7,10,12,14,16	4,6,15	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,7,10,12	4,6,13	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,7,10,12,16,17,18	4,6,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,7,10,12,18	4,6,13,15,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,7,10,12,16,17	4,6,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,7,10,12,14,17,18	4,6,13,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,7,10,12,14,16	4,6,13	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,7,10,12,14,17	4,6,13,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,7,10,12,14,16,18	4,6,13,15,18	2^{-23}

Table 0.1460 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,7,10,17,18	4,6,11,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,7,10,16	4,6,11	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,7,10,17	4,6,11,15,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,7,10,16,18	4,6,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,7,10,14	4,6,11	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,7,10,14,16,17,18	4,6,11,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,7,10,14,18	4,6,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,7,10,14,16,17	4,6,11,15,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,7,10,17	4,6,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,7,10,16,18	4,6,11,13,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,7,10,17,18	4,6,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,7,10,16	4,6,11,13,15	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,7,10,14,18	4,6,11,13,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,7,10,14,16,17	4,6,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,7,10,14	4,6,11,13,15	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,7,10,14,16,17,18	4,6,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,7,10,12	4,6,11	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,7,10,12,16,17,18	4,6,11,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,7,10,12,18	4,6,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,7,10,12,16,17	4,6,11,15,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,7,10,12,14,17,18	4,6,11,17,18	2^{-1}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,7,10,12,14,16	4,6,11	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,7,10,12,14,17	4,6,11,15,17	2^{-1}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,7,10,12,14,16,18	4,6,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,7,10,12,18	4,6,11,13,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,7,10,12,16,17	4,6,11,13,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,7,10,12	4,6,11,13,15	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,7,10,12,16,17,18	4,6,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,7,10,12,14,17	4,6,11,13,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,7,10,12,14,16,18	4,6,11,13,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,7,10,12,14,17,18	4,6,11,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,7,10,12,14,16	4,6,11,13,15	2^{-23}

Table 0.1461 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,7	4,6,9	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,7,16,17,18	4,6,9,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,7,18	4,6,9,15,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,7,16,17	4,6,9,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,7,14,17,18	4,6,9,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,7,14,16	4,6,9	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,7,14,17	4,6,9,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,7,14,16,18	4,6,9,15,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,7,18	4,6,9,13,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,7,16,17	4,6,9,13,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,7	4,6,9,13,15	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,7,16,17,18	4,6,9,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,7,14,17	4,6,9,13,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,7,14,16,18	4,6,9,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,7,14,17,18	4,6,9,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,7,14,16	4,6,9,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,7,12,17,18	4,6,9,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,7,12,16	4,6,9	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,7,12,17	4,6,9,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,7,12,16,18	4,6,9,15,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,7,12,14	4,6,9	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,7,12,14,16,17,18	4,6,9,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,7,12,14,18	4,6,9,15,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,7,12,14,16,17	4,6,9,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,12,17	4,6,9,13,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,7,12,16,18	4,6,9,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,12,17,18	4,6,9,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,7,12,16	4,6,9,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,7,12,14,18	4,6,9,13,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,7,12,14,16,17	4,6,9,13,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,7,12,14	4,6,9,13,15	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,7,12,14,16,17,18	4,6,9,13,15,17,18	2^{-23}

Table 0.1462 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,7,18	4,6,9,11,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,7,16,17	4,6,9,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,7	4,6,9,11,15	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,7,16,17,18	4,6,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,7,14,17	4,6,9,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,7,14,16,18	4,6,9,11,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,7,14,17,18	4,6,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,7,14,16	4,6,9,11,15	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,7	4,6,9,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,7,16,17,18	4,6,9,11,13,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,7,18	4,6,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,7,16,17	4,6,9,11,13,15,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,7,14,17,18	4,6,9,11,13,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,7,14,16	4,6,9,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,7,14,17	4,6,9,11,13,15,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,7,14,16,18	4,6,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,7,12,17	4,6,9,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,7,12,16,18	4,6,9,11,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,7,12,17,18	4,6,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,7,12,16	4,6,9,11,15	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,7,12,14,18	4,6,9,11,18	2^{-1}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,7,12,14,16,17	4,6,9,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,7,12,14	4,6,9,11,15	2^{-1}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,7,12,14,16,17,18	4,6,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,7,12,17,18	4,6,9,11,13,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,7,12,16	4,6,9,11,13	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,7,12,17	4,6,9,11,13,15,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,7,12,16,18	4,6,9,11,13,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,7,12,14	4,6,9,11,13	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,7,12,14,16,17,18	4,6,9,11,13,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,7,12,14,18	4,6,9,11,13,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,7,12,14,16,17	4,6,9,11,13,15,17	2^{-23}

Table 0.1463 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,7,10,17,18	4,6,9,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,7,10,16	4,6,9	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,7,10,17	4,6,9,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,7,10,16,18	4,6,9,15,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,7,10,14	4,6,9	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,7,10,14,16,17,18	4,6,9,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,7,10,14,18	4,6,9,15,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,7,10,14,16,17	4,6,9,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,7,10,17	4,6,9,13,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,7,10,16,18	4,6,9,13,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,7,10,17,18	4,6,9,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,7,10,16	4,6,9,13,15	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,7,10,14,18	4,6,9,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,7,10,14,16,17	4,6,9,13,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,7,10,14	4,6,9,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,7,10,14,16,17,18	4,6,9,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,7,10,12	4,6,9	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,7,10,12,16,17,18	4,6,9,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,7,10,12,18	4,6,9,15,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,7,10,12,16,17	4,6,9,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,7,10,12,14,17,18	4,6,9,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,7,10,12,14,16	4,6,9	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,7,10,12,14,17	4,6,9,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,7,10,12,14,16,18	4,6,9,15,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,7,10,12,18	4,6,9,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,7,10,12,16,17	4,6,9,13,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,7,10,12	4,6,9,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,7,10,12,16,17,18	4,6,9,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,7,10,12,14,17	4,6,9,13,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,7,10,12,14,16,18	4,6,9,13,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,7,10,12,14,17,18	4,6,9,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,7,10,12,14,16	4,6,9,13,15	$2^{-28.5}$

Table 0.1464 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,7,10,17	4,6,9,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,7,10,16,18	4,6,9,11,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,7,10,17,18	4,6,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,7,10,16	4,6,9,11,15	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,7,10,14,18	4,6,9,11,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,7,10,14,16,17	4,6,9,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,7,10,14	4,6,9,11,15	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,7,10,14,16,17,18	4,6,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,7,10,17,18	4,6,9,11,13,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,7,10,16	4,6,9,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,7,10,17	4,6,9,11,13,15,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,7,10,16,18	4,6,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,7,10,14	4,6,9,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,7,10,14,16,17,18	4,6,9,11,13,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,7,10,14,18	4,6,9,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,7,10,14,16,17	4,6,9,11,13,15,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,7,10,12,18	4,6,9,11,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,7,10,12,16,17	4,6,9,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,7,10,12	4,6,9,11,15	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,7,10,12,16,17,18	4,6,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,7,10,12,14,17	4,6,9,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,7,10,12,14,16,18	4,6,9,11,18	2^{-34}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,7,10,12,14,17,18	4,6,9,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,7,10,12,14,16	4,6,9,11,15	2^{-34}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,7,10,12	4,6,9,11,13	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,7,10,12,16,17,18	4,6,9,11,13,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,7,10,12,18	4,6,9,11,13,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,7,10,12,16,17	4,6,9,11,13,15,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,7,10,12,14,17,18	4,6,9,11,13,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,7,10,12,14,16	4,6,9,11,13	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,7,10,12,14,17	4,6,9,11,13,15,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,7,10,12,14,16,18	4,6,9,11,13,15,18	$2^{-28.5}$

Table 0.1465 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,7,17	4,6,8,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,7,16,18	4,6,8,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,7,17,18	4,6,8,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,7,16	4,6,8,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,7,14,18	4,6,8,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,7,14,16,17	4,6,8,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,7,14	4,6,8,15	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,7,14,16,17,18	4,6,8,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,7,17,18	4,6,8,13,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,7,16	4,6,8,13	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,7,17	4,6,8,13,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,7,16,18	4,6,8,13,15,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,7,14	4,6,8,13	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,7,14,16,17,18	4,6,8,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,7,14,18	4,6,8,13,15,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,7,14,16,17	4,6,8,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,7,12,18	4,6,8,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,7,12,16,17	4,6,8,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,7,12	4,6,8,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,7,12,16,17,18	4,6,8,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,7,12,14,17	4,6,8,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,7,12,14,16,18	4,6,8,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,7,12,14,17,18	4,6,8,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,7,12,14,16	4,6,8,15	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,7,12	4,6,8,13	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,7,12,16,17,18	4,6,8,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,7,12,18	4,6,8,13,15,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,7,12,16,17	4,6,8,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,7,12,14,17,18	4,6,8,13,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,7,12,14,16	4,6,8,13	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,7,12,14,17	4,6,8,13,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,7,12,14,16,18	4,6,8,13,15,18	2^{-12}

Table 0.1466 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,7,17,18	4,6,8,11,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,7,16	4,6,8,11	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,7,17	4,6,8,11,15,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,7,16,18	4,6,8,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,7,14	4,6,8,11	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,7,14,16,17,18	4,6,8,11,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,7,14,18	4,6,8,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,7,14,16,17	4,6,8,11,15,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,7,17	4,6,8,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,7,16,18	4,6,8,11,13,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,7,17,18	4,6,8,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,7,16	4,6,8,11,13,15	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,7,14,18	4,6,8,11,13,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,7,14,16,17	4,6,8,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,7,14	4,6,8,11,13,15	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,7,14,16,17,18	4,6,8,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,7,12	4,6,8,11	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,7,12,16,17,18	4,6,8,11,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,7,12,18	4,6,8,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,7,12,16,17	4,6,8,11,15,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,7,12,14,17,18	4,6,8,11,17,18	2^{-34}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,7,12,14,16	4,6,8,11	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,7,12,14,17	4,6,8,11,15,17	2^{-34}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,7,12,14,16,18	4,6,8,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,7,12,18	4,6,8,11,13,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,7,12,16,17	4,6,8,11,13,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,7,12	4,6,8,11,13,15	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,7,12,16,17,18	4,6,8,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,7,12,14,17	4,6,8,11,13,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,7,12,14,16,18	4,6,8,11,13,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,7,12,14,17,18	4,6,8,11,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,7,12,14,16	4,6,8,11,13,15	2^{-12}

Table 0.1467 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,7,10,18	4,6,8,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,7,10,16,17	4,6,8,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,7,10	4,6,8,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,7,10,16,17,18	4,6,8,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,7,10,14,17	4,6,8,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,7,10,14,16,18	4,6,8,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,7,10,14,17,18	4,6,8,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,7,10,14,16	4,6,8,15	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,7,10	4,6,8,13	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,7,10,16,17,18	4,6,8,13,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,7,10,18	4,6,8,13,15,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,7,10,16,17	4,6,8,13,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,7,10,14,17,18	4,6,8,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,7,10,14,16	4,6,8,13	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,7,10,14,17	4,6,8,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,7,10,14,16,18	4,6,8,13,15,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,7,10,12,17	4,6,8,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,7,10,12,16,18	4,6,8,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,7,10,12,17,18	4,6,8,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,7,10,12,16	4,6,8,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,7,10,12,14,18	4,6,8,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,7,10,12,14,16,17	4,6,8,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,7,10,12,14	4,6,8,15	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,7,10,12,14,16,17,18	4,6,8,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,7,10,12,17,18	4,6,8,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,10,12,16	4,6,8,13	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,7,10,12,17	4,6,8,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,10,12,16,18	4,6,8,13,15,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,7,10,12,14	4,6,8,13	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,7,10,12,14,16,17,18	4,6,8,13,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,7,10,12,14,18	4,6,8,13,15,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,7,10,12,14,16,17	4,6,8,13,15,17	$2^{-6.5}$

Table 0.1469 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,7,17,18	4,6,8,9,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,7,16	4,6,8,9	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,7,17	4,6,8,9,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,7,16,18	4,6,8,9,15,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,7,14	4,6,8,9	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,7,14,16,17,18	4,6,8,9,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,7,14,18	4,6,8,9,15,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,7,14,16,17	4,6,8,9,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,7,17	4,6,8,9,13,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,7,16,18	4,6,8,9,13,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,7,17,18	4,6,8,9,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,7,16	4,6,8,9,13,15	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,7,14,18	4,6,8,9,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,7,14,16,17	4,6,8,9,13,17	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,7,14	4,6,8,9,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,7,14,16,17,18	4,6,8,9,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,7,12	4,6,8,9	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,7,12,16,17,18	4,6,8,9,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,7,12,18	4,6,8,9,15,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,7,12,16,17	4,6,8,9,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,7,12,14,17,18	4,6,8,9,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,7,12,14,16	4,6,8,9	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,7,12,14,17	4,6,8,9,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,7,12,14,16,18	4,6,8,9,15,18	2^{-12}
$(1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,7,12,18	4,6,8,9,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,7,12,16,17	4,6,8,9,13,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,7,12	4,6,8,9,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,7,12,16,17,18	4,6,8,9,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,7,12,14,17	4,6,8,9,13,17	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,7,12,14,16,18	4,6,8,9,13,18	$2^{-6.5}$
$(1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,7,12,14,17,18	4,6,8,9,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,7,12,14,16	4,6,8,9,13,15	$2^{-6.5}$

Table 0.1473 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,17	4,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,16,18	4,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,17,18	4,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,16	4,15	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,14,18	4,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,14,16,17	4,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,14	4,15	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,14,16,17,18	4,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,17,18	4,13,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,16	4,13	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,17	4,13,15,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,16,18	4,13,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,14	4,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,14,16,17,18	4,13,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,14,18	4,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,14,16,17	4,13,15,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,12,18	4,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,12,16,17	4,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,12	4,15	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,12,16,17,18	4,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,12,14,17	4,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,12,14,16,18	4,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,12,14,17,18	4,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,12,14,16	4,15	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,12	4,13	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,12,16,17,18	4,13,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,12,18	4,13,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,12,16,17	4,13,15,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,12,14,17,18	4,13,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,12,14,16	4,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,12,14,17	4,13,15,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,12,14,16,18	4,13,15,18	$2^{-17.5}$

Table 0.1474 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,17,18	4,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,16	4,11	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,17	4,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,16,18	4,11,15,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,14	4,11	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,14,16,17,18	4,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,14,18	4,11,15,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,14,16,17	4,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,17	4,11,13,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,16,18	4,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,17,18	4,11,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,16	4,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,14,18	4,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,14,16,17	4,11,13,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,14	4,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,14,16,17,18	4,11,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,12	4,11	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,12,16,17,18	4,11,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,12,18	4,11,15,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,12,16,17	4,11,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,12,14,17,18	4,11,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,12,14,16	4,11	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,12,14,17	4,11,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,12,14,16,18	4,11,15,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,12,18	4,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,12,16,17	4,11,13,17	2^{-34}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,12	4,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,12,16,17,18	4,11,13,15,17,18	2^{-34}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,12,14,17	4,11,13,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,12,14,16,18	4,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,12,14,17,18	4,11,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,12,14,16	4,11,13,15	$2^{-17.5}$

Table 0.1475 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,10,18	4,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,10,16,17	4,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,10	4,15	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,10,16,17,18	4,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,10,14,17	4,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,10,14,16,18	4,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,10,14,17,18	4,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,10,14,16	4,15	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,10	4,13	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,10,16,17,18	4,13,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,10,18	4,13,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,10,16,17	4,13,15,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,10,14,17,18	4,13,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,10,14,16	4,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,10,14,17	4,13,15,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,10,14,16,18	4,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,10,12,17	4,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,10,12,16,18	4,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,10,12,17,18	4,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,10,12,16	4,15	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,10,12,14,18	4,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,10,12,14,16,17	4,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,10,12,14	4,15	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,10,12,14,16,17,18	4,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,10,12,17,18	4,13,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,10,12,16	4,13	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,10,12,17	4,13,15,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,10,12,16,18	4,13,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,10,12,14	4,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,10,12,14,16,17,18	4,13,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,10,12,14,18	4,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,10,12,14,16,17	4,13,15,17	2^{-12}

Table 0.1476 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,10	4,11	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,10,16,17,18	4,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,10,18	4,11,15,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,10,16,17	4,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,10,14,17,18	4,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,10,14,16	4,11	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,10,14,17	4,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,10,14,16,18	4,11,15,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,10,18	4,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,10,16,17	4,11,13,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,10	4,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,10,16,17,18	4,11,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,10,14,17	4,11,13,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,10,14,16,18	4,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,10,14,17,18	4,11,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,10,14,16	4,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,10,12,17,18	4,11,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,10,12,16	4,11	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,10,12,17	4,11,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,10,12,16,18	4,11,15,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,10,12,14	4,11	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,10,12,14,16,17,18	4,11,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,10,12,14,18	4,11,15,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,10,12,14,16,17	4,11,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,10,12,17	4,11,13,17	2^{-1}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,10,12,16,18	4,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,10,12,17,18	4,11,13,15,17,18	2^{-1}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,10,12,16	4,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,10,12,14,18	4,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,10,12,14,16,17	4,11,13,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,10,12,14	4,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,10,12,14,16,17,18	4,11,13,15,17,18	2^{-12}

Table 0.1477 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,17,18	4,9,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,16	4,9	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,17	4,9,15,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,16,18	4,9,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,14	4,9	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,14,16,17,18	4,9,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,14,18	4,9,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,14,16,17	4,9,15,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,17	4,9,13,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,16,18	4,9,13,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,17,18	4,9,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,16	4,9,13,15	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,14,18	4,9,13,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,14,16,17	4,9,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,14	4,9,13,15	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,14,16,17,18	4,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,12	4,9	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,12,16,17,18	4,9,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,12,18	4,9,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,12,16,17	4,9,15,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,12,14,17,18	4,9,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,12,14,16	4,9	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,12,14,17	4,9,15,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,12,14,16,18	4,9,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,12,18	4,9,13,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,12,16,17	4,9,13,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,12	4,9,13,15	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,12,16,17,18	4,9,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,12,14,17	4,9,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,12,14,16,18	4,9,13,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,12,14,17,18	4,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,12,14,16	4,9,13,15	2^{-12}

Table 0.1478 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,17	4,9,11,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,16,18	4,9,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,17,18	4,9,11,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,16	4,9,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,14,18	4,9,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,14,16,17	4,9,11,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,14	4,9,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,14,16,17,18	4,9,11,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,17,18	4,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,16	4,9,11,13	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,17	4,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,16,18	4,9,11,13,15,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,14	4,9,11,13	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,14,16,17,18	4,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,14,18	4,9,11,13,15,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,14,16,17	4,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,12,18	4,9,11,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,12,16,17	4,9,11,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,12	4,9,11,15	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,12,16,17,18	4,9,11,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,12,14,17	4,9,11,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,12,14,16,18	4,9,11,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,12,14,17,18	4,9,11,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,12,14,16	4,9,11,15	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,12	4,9,11,13	2^{-1}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,12,16,17,18	4,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,12,18	4,9,11,13,15,18	2^{-1}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,12,16,17	4,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,12,14,17,18	4,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,12,14,16	4,9,11,13	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,12,14,17	4,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,12,14,16,18	4,9,11,13,15,18	2^{-12}

Table 0.1479 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,10	4,9	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,10,16,17,18	4,9,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,10,18	4,9,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,10,16,17	4,9,15,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,10,14,17,18	4,9,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,10,14,16	4,9	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,10,14,17	4,9,15,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,10,14,16,18	4,9,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,10,18	4,9,13,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,10,16,17	4,9,13,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,10	4,9,13,15	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,10,16,17,18	4,9,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,10,14,17	4,9,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,10,14,16,18	4,9,13,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,10,14,17,18	4,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,10,14,16	4,9,13,15	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,10,12,17,18	4,9,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,10,12,16	4,9	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,10,12,17	4,9,15,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,10,12,16,18	4,9,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,10,12,14	4,9	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,10,12,14,16,17,18	4,9,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,10,12,14,18	4,9,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,10,12,14,16,17	4,9,15,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,10,12,17	4,9,13,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,10,12,16,18	4,9,13,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,10,12,17,18	4,9,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,10,12,16	4,9,13,15	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,10,12,14,18	4,9,13,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,10,12,14,16,17	4,9,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,10,12,14	4,9,13,15	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,10,12,14,16,17,18	4,9,13,15,17,18	$2^{-17.5}$

Table 0.1480 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,10,18	4,9,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,10,16,17	4,9,11,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,10	4,9,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,10,16,17,18	4,9,11,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,10,14,17	4,9,11,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,10,14,16,18	4,9,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,10,14,17,18	4,9,11,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,10,14,16	4,9,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,10	4,9,11,13	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,10,16,17,18	4,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,10,18	4,9,11,13,15,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,10,16,17	4,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,10,14,17,18	4,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,10,14,16	4,9,11,13	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,10,14,17	4,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,10,14,16,18	4,9,11,13,15,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,10,12,17	4,9,11,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,10,12,16,18	4,9,11,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,10,12,17,18	4,9,11,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,10,12,16	4,9,11,15	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,10,12,14,18	4,9,11,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,10,12,14,16,17	4,9,11,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,10,12,14	4,9,11,15	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,10,12,14,16,17,18	4,9,11,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,10,12,17,18	4,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,10,12,16	4,9,11,13	2^{-34}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,10,12,17	4,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,10,12,16,18	4,9,11,13,15,18	2^{-34}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,10,12,14	4,9,11,13	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,10,12,14,16,17,18	4,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,10,12,14,18	4,9,11,13,15,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,10,12,14,16,17	4,9,11,13,15,17	$2^{-17.5}$

Table 0.1481 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,18	4,8,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,16,17	4,8,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,5	4,8,15	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,16,17,18	4,8,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,14,17	4,8,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,14,16,18	4,8,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,14,17,18	4,8,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,14,16	4,8,15	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,5	4,8,13	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,16,17,18	4,8,13,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,18	4,8,13,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,16,17	4,8,13,15,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,14,17,18	4,8,13,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,14,16	4,8,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,14,17	4,8,13,15,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,14,16,18	4,8,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,12,17	4,8,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,12,16,18	4,8,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,12,17,18	4,8,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,12,16	4,8,15	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,12,14,18	4,8,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,12,14,16,17	4,8,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,12,14	4,8,15	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,12,14,16,17,18	4,8,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,12,17,18	4,8,13,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,12,16	4,8,13	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,12,17	4,8,13,15,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,12,16,18	4,8,13,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,12,14	4,8,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,12,14,16,17,18	4,8,13,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,12,14,18	4,8,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,12,14,16,17	4,8,13,15,17	2^{-23}

Table 0.1482 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,5	4,8,11	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,16,17,18	4,8,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,18	4,8,11,15,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,16,17	4,8,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,14,17,18	4,8,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,14,16	4,8,11	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,14,17	4,8,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,14,16,18	4,8,11,15,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,18	4,8,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,16,17	4,8,11,13,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,5	4,8,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,16,17,18	4,8,11,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,14,17	4,8,11,13,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,14,16,18	4,8,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,14,17,18	4,8,11,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,14,16	4,8,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,12,17,18	4,8,11,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,12,16	4,8,11	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,12,17	4,8,11,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,12,16,18	4,8,11,15,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,12,14	4,8,11	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,12,14,16,17,18	4,8,11,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,12,14,18	4,8,11,15,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,12,14,16,17	4,8,11,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,12,17	4,8,11,13,17	2^{-34}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,12,16,18	4,8,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,12,17,18	4,8,11,13,15,17,18	2^{-34}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,12,16	4,8,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,12,14,18	4,8,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,12,14,16,17	4,8,11,13,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,12,14	4,8,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,12,14,16,17,18	4,8,11,13,15,17,18	2^{-23}

Table 0.1483 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,10,17	4,8,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,10,16,18	4,8,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,10,17,18	4,8,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,10,16	4,8,15	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,10,14,18	4,8,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,10,14,16,17	4,8,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,10,14	4,8,15	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,10,14,16,17,18	4,8,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,10,17,18	4,8,13,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,10,16	4,8,13	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,10,17	4,8,13,15,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,10,16,18	4,8,13,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,10,14	4,8,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,10,14,16,17,18	4,8,13,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,10,14,18	4,8,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,10,14,16,17	4,8,13,15,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,10,12,18	4,8,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,10,12,16,17	4,8,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,10,12	4,8,15	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,10,12,16,17,18	4,8,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,10,12,14,17	4,8,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,10,12,14,16,18	4,8,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,10,12,14,17,18	4,8,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,10,12,14,16	4,8,15	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,10,12	4,8,13	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,10,12,16,17,18	4,8,13,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,10,12,18	4,8,13,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,10,12,16,17	4,8,13,15,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,10,12,14,17,18	4,8,13,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,10,12,14,16	4,8,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,10,12,14,17	4,8,13,15,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,10,12,14,16,18	4,8,13,15,18	$2^{-17.5}$

Table 0.1484 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,10,17,18	4,8,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,10,16	4,8,11	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,10,17	4,8,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,10,16,18	4,8,11,15,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,10,14	4,8,11	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,10,14,16,17,18	4,8,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,10,14,18	4,8,11,15,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,10,14,16,17	4,8,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,10,17	4,8,11,13,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,10,16,18	4,8,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,10,17,18	4,8,11,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,10,16	4,8,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,10,14,18	4,8,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,10,14,16,17	4,8,11,13,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,10,14	4,8,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,10,14,16,17,18	4,8,11,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,10,12	4,8,11	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,10,12,16,17,18	4,8,11,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,10,12,18	4,8,11,15,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,10,12,16,17	4,8,11,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,10,12,14,17,18	4,8,11,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,10,12,14,16	4,8,11	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,10,12,14,17	4,8,11,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,10,12,14,16,18	4,8,11,15,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,10,12,18	4,8,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,10,12,16,17	4,8,11,13,17	2^{-1}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,10,12	4,8,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,10,12,16,17,18	4,8,11,13,15,17,18	2^{-1}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,10,12,14,17	4,8,11,13,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,10,12,14,16,18	4,8,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,10,12,14,17,18	4,8,11,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,10,12,14,16	4,8,11,13,15	$2^{-17.5}$

Table 0.1485 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,5	4,8,9	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,16,17,18	4,8,9,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,18	4,8,9,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,16,17	4,8,9,15,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,14,17,18	4,8,9,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,14,16	4,8,9	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,14,17	4,8,9,15,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,14,16,18	4,8,9,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,18	4,8,9,13,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,16,17	4,8,9,13,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,5	4,8,9,13,15	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,16,17,18	4,8,9,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,14,17	4,8,9,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,14,16,18	4,8,9,13,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,14,17,18	4,8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,14,16	4,8,9,13,15	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,12,17,18	4,8,9,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,12,16	4,8,9	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,12,17	4,8,9,15,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,12,16,18	4,8,9,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,12,14	4,8,9	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,12,14,16,17,18	4,8,9,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,12,14,18	4,8,9,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,12,14,16,17	4,8,9,15,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,12,17	4,8,9,13,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,12,16,18	4,8,9,13,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,12,17,18	4,8,9,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,12,16	4,8,9,13,15	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,12,14,18	4,8,9,13,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,12,14,16,17	4,8,9,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,12,14	4,8,9,13,15	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,12,14,16,17,18	4,8,9,13,15,17,18	$2^{-17.5}$

Table 0.1486 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,18	4,8,9,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,16,17	4,8,9,11,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,5	4,8,9,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,16,17,18	4,8,9,11,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,14,17	4,8,9,11,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,14,16,18	4,8,9,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,14,17,18	4,8,9,11,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,14,16	4,8,9,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,5	4,8,9,11,13	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,16,17,18	4,8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,18	4,8,9,11,13,15,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,16,17	4,8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,14,17,18	4,8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,14,16	4,8,9,11,13	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,14,17	4,8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,14,16,18	4,8,9,11,13,15,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,12,17	4,8,9,11,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,12,16,18	4,8,9,11,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,12,17,18	4,8,9,11,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,12,16	4,8,9,11,15	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,12,14,18	4,8,9,11,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,12,14,16,17	4,8,9,11,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,12,14	4,8,9,11,15	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,12,14,16,17,18	4,8,9,11,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,12,17,18	4,8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,12,16	4,8,9,11,13	2^{-1}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,12,17	4,8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,12,16,18	4,8,9,11,13,15,18	2^{-1}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,12,14	4,8,9,11,13	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,12,14,16,17,18	4,8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,12,14,18	4,8,9,11,13,15,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,12,14,16,17	4,8,9,11,13,15,17	$2^{-17.5}$

Table 0.1487 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,10,17,18	4,8,9,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,10,16	4,8,9	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,10,17	4,8,9,15,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,10,16,18	4,8,9,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,10,14	4,8,9	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,10,14,16,17,18	4,8,9,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,10,14,18	4,8,9,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,10,14,16,17	4,8,9,15,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,10,17	4,8,9,13,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,10,16,18	4,8,9,13,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,10,17,18	4,8,9,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,10,16	4,8,9,13,15	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,10,14,18	4,8,9,13,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,10,14,16,17	4,8,9,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,10,14	4,8,9,13,15	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,10,14,16,17,18	4,8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,10,12	4,8,9	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,10,12,16,17,18	4,8,9,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,10,12,18	4,8,9,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,10,12,16,17	4,8,9,15,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,10,12,14,17,18	4,8,9,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,10,12,14,16	4,8,9	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,10,12,14,17	4,8,9,15,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,10,12,14,16,18	4,8,9,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,10,12,18	4,8,9,13,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,10,12,16,17	4,8,9,13,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,10,12	4,8,9,13,15	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,10,12,16,17,18	4,8,9,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,10,12,14,17	4,8,9,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,10,12,14,16,18	4,8,9,13,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,10,12,14,17,18	4,8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,10,12,14,16	4,8,9,13,15	2^{-23}

Table 0.1488 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,10,17	4,8,9,11,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,10,16,18	4,8,9,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,10,17,18	4,8,9,11,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,10,16	4,8,9,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,10,14,18	4,8,9,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,10,14,16,17	4,8,9,11,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,10,14	4,8,9,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,10,14,16,17,18	4,8,9,11,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,10,17,18	4,8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,10,16	4,8,9,11,13	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,10,17	4,8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,10,16,18	4,8,9,11,13,15,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,10,14	4,8,9,11,13	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,10,14,16,17,18	4,8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,10,14,18	4,8,9,11,13,15,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,10,14,16,17	4,8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,10,12,18	4,8,9,11,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,10,12,16,17	4,8,9,11,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,10,12	4,8,9,11,15	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,10,12,16,17,18	4,8,9,11,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,10,12,14,17	4,8,9,11,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,10,12,14,16,18	4,8,9,11,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,10,12,14,17,18	4,8,9,11,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,10,12,14,16	4,8,9,11,15	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,10,12	4,8,9,11,13	2^{-34}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,10,12,16,17,18	4,8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,10,12,18	4,8,9,11,13,15,18	2^{-34}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,10,12,16,17	4,8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,10,12,14,17,18	4,8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,10,12,14,16	4,8,9,11,13	2^{-23}
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,10,12,14,17	4,8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,10,12,14,16,18	4,8,9,11,13,15,18	2^{-23}

Table 0.1489 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,7,17,18	4,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,7,16	4	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,7,17	4,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,7,16,18	4,15,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,7,14	4	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,7,14,16,17,18	4,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,7,14,18	4,15,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,7,14,16,17	4,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,7,17	4,13,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,7,16,18	4,13,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,7,17,18	4,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,7,16	4,13,15	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,7,14,18	4,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,7,14,16,17	4,13,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,7,14	4,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,7,14,16,17,18	4,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,7,12	4	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,7,12,16,17,18	4,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,7,12,18	4,15,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,7,12,16,17	4,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,7,12,14,17,18	4,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,7,12,14,16	4	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,7,12,14,17	4,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,7,12,14,16,18	4,15,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,7,12,18	4,13,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,7,12,16,17	4,13,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,7,12	4,13,15	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,7,12,16,17,18	4,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,7,12,14,17	4,13,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,7,12,14,16,18	4,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,7,12,14,17,18	4,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,7,12,14,16	4,13,15	$2^{-17.5}$

Table 0.1490 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,7,17	4,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,7,16,18	4,11,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,7,17,18	4,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,7,16	4,11,15	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,7,14,18	4,11,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,7,14,16,17	4,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,7,14	4,11,15	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,7,14,16,17,18	4,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,7,17,18	4,11,13,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,7,16	4,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,7,17	4,11,13,15,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,7,16,18	4,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,7,14	4,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,7,14,16,17,18	4,11,13,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,7,14,18	4,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,7,14,16,17	4,11,13,15,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,7,12,18	4,11,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,7,12,16,17	4,11,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,7,12	4,11,15	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,7,12,16,17,18	4,11,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,7,12,14,17	4,11,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,7,12,14,16,18	4,11,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,7,12,14,17,18	4,11,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,7,12,14,16	4,11,15	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,7,12	4,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7,12,16,17,18	4,11,13,17,18	2^{-34}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,7,12,18	4,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7,12,16,17	4,11,13,15,17	2^{-34}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,7,12,14,17,18	4,11,13,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,7,12,14,16	4,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,7,12,14,17	4,11,13,15,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,7,12,14,16,18	4,11,13,15,18	$2^{-17.5}$

Table 0.1491 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,7,10	4	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,10,16,17,18	4,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,7,10,18	4,15,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,10,16,17	4,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,10,14,17,18	4,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,7,10,14,16	4	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,10,14,17	4,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,7,10,14,16,18	4,15,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,7,10,18	4,13,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,7,10,16,17	4,13,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,7,10	4,13,15	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,7,10,16,17,18	4,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,7,10,14,17	4,13,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,7,10,14,16,18	4,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,7,10,14,17,18	4,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,7,10,14,16	4,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,7,10,12,17,18	4,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,7,10,12,16	4	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,7,10,12,17	4,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,7,10,12,16,18	4,15,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,12,14	4	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,7,10,12,14,16,17,18	4,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,12,14,18	4,15,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,7,10,12,14,16,17	4,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,7,10,12,17	4,13,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,7,10,12,16,18	4,13,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,7,10,12,17,18	4,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,7,10,12,16	4,13,15	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,12,14,18	4,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,7,10,12,14,16,17	4,13,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,12,14	4,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,7,10,12,14,16,17,18	4,13,15,17,18	2^{-12}

Table 0.1492 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,10,18	4,11,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,16,17	4,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,10	4,11,15	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,16,17,18	4,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7,10,14,17	4,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,7,10,14,16,18	4,11,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7,10,14,17,18	4,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,7,10,14,16	4,11,15	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,10	4,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,16,17,18	4,11,13,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,10,18	4,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,7,10,16,17	4,11,13,15,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,7,10,14,17,18	4,11,13,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,7,10,14,16	4,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,7,10,14,17	4,11,13,15,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,7,10,14,16,18	4,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7,10,12,17	4,11,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,7,10,12,16,18	4,11,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7,10,12,17,18	4,11,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,7,10,12,16	4,11,15	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,7,10,12,14,18	4,11,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,7,10,12,14,16,17	4,11,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,7,10,12,14	4,11,15	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,12,14,16,17,18	4,11,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,7,10,12,17,18	4,11,13,17,18	2^{-1}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,7,10,12,16	4,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,7,10,12,17	4,11,13,15,17	2^{-1}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,7,10,12,16,18	4,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,7,10,12,14	4,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,7,10,12,14,16,17,18	4,11,13,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,7,10,12,14,18	4,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,7,10,12,14,16,17	4,11,13,15,17	2^{-12}

Table 0.1493 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,7,17	4,9,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,7,16,18	4,9,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,7,17,18	4,9,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,7,16	4,9,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,7,14,18	4,9,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,7,14,16,17	4,9,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,7,14	4,9,15	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,7,14,16,17,18	4,9,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,7,17,18	4,9,13,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,7,16	4,9,13	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,7,17	4,9,13,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,7,16,18	4,9,13,15,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,7,14	4,9,13	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,7,14,16,17,18	4,9,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,7,14,18	4,9,13,15,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,7,14,16,17	4,9,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,7,12,18	4,9,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,7,12,16,17	4,9,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,7,12	4,9,15	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,7,12,16,17,18	4,9,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,7,12,14,17	4,9,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,7,12,14,16,18	4,9,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,7,12,14,17,18	4,9,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,7,12,14,16	4,9,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,7,12	4,9,13	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,7,12,16,17,18	4,9,13,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,7,12,18	4,9,13,15,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,7,12,16,17	4,9,13,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,7,12,14,17,18	4,9,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,7,12,14,16	4,9,13	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,7,12,14,17	4,9,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,7,12,14,16,18	4,9,13,15,18	2^{-12}

Table 0.1494 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,7,17,18	4,9,11,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,7,16	4,9,11	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,7,17	4,9,11,15,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,7,16,18	4,9,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,7,14	4,9,11	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,7,14,16,17,18	4,9,11,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,7,14,18	4,9,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,7,14,16,17	4,9,11,15,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,7,17	4,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,7,16,18	4,9,11,13,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,7,17,18	4,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,7,16	4,9,11,13,15	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,7,14,18	4,9,11,13,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,7,14,16,17	4,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,7,14	4,9,11,13,15	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,7,14,16,17,18	4,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,7,12	4,9,11	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7,12,16,17,18	4,9,11,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,7,12,18	4,9,11,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7,12,16,17	4,9,11,15,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,7,12,14,17,18	4,9,11,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,7,12,14,16	4,9,11	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,7,12,14,17	4,9,11,15,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,7,12,14,16,18	4,9,11,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,7,12,18	4,9,11,13,18	2^{-1}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,7,12,16,17	4,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,7,12	4,9,11,13,15	2^{-1}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,7,12,16,17,18	4,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,7,12,14,17	4,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,7,12,14,16,18	4,9,11,13,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,7,12,14,17,18	4,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,7,12,14,16	4,9,11,13,15	2^{-12}

Table 0.1495 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,7,10,18	4,9,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,7,10,16,17	4,9,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,7,10	4,9,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,7,10,16,17,18	4,9,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,7,10,14,17	4,9,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,7,10,14,16,18	4,9,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,7,10,14,17,18	4,9,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,7,10,14,16	4,9,15	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,7,10	4,9,13	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,7,10,16,17,18	4,9,13,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,7,10,18	4,9,13,15,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,7,10,16,17	4,9,13,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,7,10,14,17,18	4,9,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,7,10,14,16	4,9,13	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,7,10,14,17	4,9,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,7,10,14,16,18	4,9,13,15,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,7,10,12,17	4,9,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,7,10,12,16,18	4,9,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,7,10,12,17,18	4,9,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,7,10,12,16	4,9,15	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,7,10,12,14,18	4,9,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,7,10,12,14,16,17	4,9,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,7,10,12,14	4,9,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,7,10,12,14,16,17,18	4,9,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,7,10,12,17,18	4,9,13,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,7,10,12,16	4,9,13	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,7,10,12,17	4,9,13,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,7,10,12,16,18	4,9,13,15,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,7,10,12,14	4,9,13	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,7,10,12,14,16,17,18	4,9,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,7,10,12,14,18	4,9,13,15,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,7,10,12,14,16,17	4,9,13,15,17	$2^{-17.5}$

Table 0.1496 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,7,10	4,9,11	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,7,10,16,17,18	4,9,11,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,7,10,18	4,9,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,7,10,16,17	4,9,11,15,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,7,10,14,17,18	4,9,11,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,7,10,14,16	4,9,11	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,7,10,14,17	4,9,11,15,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,7,10,14,16,18	4,9,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,7,10,18	4,9,11,13,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,7,10,16,17	4,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,7,10	4,9,11,13,15	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,7,10,16,17,18	4,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,7,10,14,17	4,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,7,10,14,16,18	4,9,11,13,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,7,10,14,17,18	4,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,7,10,14,16	4,9,11,13,15	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,7,10,12,17,18	4,9,11,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,7,10,12,16	4,9,11	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,7,10,12,17	4,9,11,15,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,7,10,12,16,18	4,9,11,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,7,10,12,14	4,9,11	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,7,10,12,14,16,17,18	4,9,11,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,7,10,12,14,18	4,9,11,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,7,10,12,14,16,17	4,9,11,15,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,7,10,12,17	4,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,7,10,12,16,18	4,9,11,13,18	2^{-34}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,7,10,12,17,18	4,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,7,10,12,16	4,9,11,13,15	2^{-34}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,7,10,12,14,18	4,9,11,13,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,7,10,12,14,16,17	4,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,7,10,12,14	4,9,11,13,15	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,7,10,12,14,16,17,18	4,9,11,13,15,17,18	$2^{-17.5}$

Table 0.1497 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,7	4,8	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,7,16,17,18	4,8,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,7,18	4,8,15,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,7,16,17	4,8,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,7,14,17,18	4,8,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,7,14,16	4,8	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,7,14,17	4,8,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,7,14,16,18	4,8,15,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,7,18	4,8,13,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,7,16,17	4,8,13,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,7	4,8,13,15	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,7,16,17,18	4,8,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,7,14,17	4,8,13,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,7,14,16,18	4,8,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,7,14,17,18	4,8,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,7,14,16	4,8,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,7,12,17,18	4,8,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,7,12,16	4,8	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,7,12,17	4,8,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,7,12,16,18	4,8,15,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,7,12,14	4,8	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,7,12,14,16,17,18	4,8,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,7,12,14,18	4,8,15,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,7,12,14,16,17	4,8,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,7,12,17	4,8,13,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,7,12,16,18	4,8,13,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,7,12,17,18	4,8,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,7,12,16	4,8,13,15	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,7,12,14,18	4,8,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,7,12,14,16,17	4,8,13,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,7,12,14	4,8,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,7,12,14,16,17,18	4,8,13,15,17,18	2^{-23}

Table 0.1498 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,7,18	4,8,11,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,7,16,17	4,8,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,7	4,8,11,15	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,7,16,17,18	4,8,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,7,14,17	4,8,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,7,14,16,18	4,8,11,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,7,14,17,18	4,8,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,7,14,16	4,8,11,15	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,7	4,8,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,7,16,17,18	4,8,11,13,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,7,18	4,8,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,7,16,17	4,8,11,13,15,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,7,14,17,18	4,8,11,13,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,7,14,16	4,8,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,7,14,17	4,8,11,13,15,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,7,14,16,18	4,8,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,7,12,17	4,8,11,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,7,12,16,18	4,8,11,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,7,12,17,18	4,8,11,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,7,12,16	4,8,11,15	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,7,12,14,18	4,8,11,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,7,12,14,16,17	4,8,11,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,7,12,14	4,8,11,15	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,7,12,14,16,17,18	4,8,11,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,7,12,17,18	4,8,11,13,17,18	2^{-34}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,7,12,16	4,8,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,7,12,17	4,8,11,13,15,17	2^{-34}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,7,12,16,18	4,8,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,7,12,14	4,8,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,7,12,14,16,17,18	4,8,11,13,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,7,12,14,18	4,8,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,7,12,14,16,17	4,8,11,13,15,17	2^{-23}

Table 0.1499 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,7,10,17,18	4,8,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,7,10,16	4,8	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,7,10,17	4,8,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,7,10,16,18	4,8,15,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,7,10,14	4,8	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,7,10,14,16,17,18	4,8,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,7,10,14,18	4,8,15,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,7,10,14,16,17	4,8,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,7,10,17	4,8,13,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,7,10,16,18	4,8,13,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,7,10,17,18	4,8,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,7,10,16	4,8,13,15	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,7,10,14,18	4,8,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,7,10,14,16,17	4,8,13,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,7,10,14	4,8,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,7,10,14,16,17,18	4,8,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,12	4,8	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10,12,16,17,18	4,8,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,12,18	4,8,15,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10,12,16,17	4,8,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,7,10,12,14,17,18	4,8,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,7,10,12,14,16	4,8	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,7,10,12,14,17	4,8,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,7,10,12,14,16,18	4,8,15,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,12,18	4,8,13,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10,12,16,17	4,8,13,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,12	4,8,13,15	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10,12,16,17,18	4,8,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,7,10,12,14,17	4,8,13,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,7,10,12,14,16,18	4,8,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,7,10,12,14,17,18	4,8,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,7,10,12,14,16	4,8,13,15	$2^{-17.5}$

Table 0.1500 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,7,10,17	4,8,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,7,10,16,18	4,8,11,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,7,10,17,18	4,8,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,7,10,16	4,8,11,15	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,7,10,14,18	4,8,11,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,7,10,14,16,17	4,8,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,7,10,14	4,8,11,15	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,7,10,14,16,17,18	4,8,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,7,10,17,18	4,8,11,13,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,7,10,16	4,8,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,7,10,17	4,8,11,13,15,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,7,10,16,18	4,8,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,7,10,14	4,8,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,7,10,14,16,17,18	4,8,11,13,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,7,10,14,18	4,8,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,7,10,14,16,17	4,8,11,13,15,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7,10,12,18	4,8,11,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,7,10,12,16,17	4,8,11,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7,10,12	4,8,11,15	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,7,10,12,16,17,18	4,8,11,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,7,10,12,14,17	4,8,11,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,7,10,12,14,16,18	4,8,11,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,7,10,12,14,17,18	4,8,11,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,7,10,12,14,16	4,8,11,15	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,7,10,12	4,8,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,7,10,12,16,17,18	4,8,11,13,17,18	2^{-1}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,7,10,12,18	4,8,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,7,10,12,16,17	4,8,11,13,15,17	2^{-1}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,7,10,12,14,17,18	4,8,11,13,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,7,10,12,14,16	4,8,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,7,10,12,14,17	4,8,11,13,15,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,7,10,12,14,16,18	4,8,11,13,15,18	$2^{-17.5}$

Table 0.1501 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,18	4,8,9,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,7,16,17	4,8,9,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7	4,8,9,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,7,16,17,18	4,8,9,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,7,14,17	4,8,9,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,14,16,18	4,8,9,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,7,14,17,18	4,8,9,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,14,16	4,8,9,15	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,7	4,8,9,13	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,7,16,17,18	4,8,9,13,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,7,18	4,8,9,13,15,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,7,16,17	4,8,9,13,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,7,14,17,18	4,8,9,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,7,14,16	4,8,9,13	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,7,14,17	4,8,9,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,7,14,16,18	4,8,9,13,15,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,7,12,17	4,8,9,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,7,12,16,18	4,8,9,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,7,12,17,18	4,8,9,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,7,12,16	4,8,9,15	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,7,12,14,18	4,8,9,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,7,12,14,16,17	4,8,9,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,7,12,14	4,8,9,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,7,12,14,16,17,18	4,8,9,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,7,12,17,18	4,8,9,13,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,7,12,16	4,8,9,13	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,7,12,17	4,8,9,13,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,7,12,16,18	4,8,9,13,15,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,7,12,14	4,8,9,13	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,7,12,14,16,17,18	4,8,9,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,7,12,14,18	4,8,9,13,15,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,7,12,14,16,17	4,8,9,13,15,17	$2^{-17.5}$

Table 0.1502 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,7	4,8,9,11	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,7,16,17,18	4,8,9,11,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,7,18	4,8,9,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,7,16,17	4,8,9,11,15,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,7,14,17,18	4,8,9,11,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,7,14,16	4,8,9,11	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,7,14,17	4,8,9,11,15,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,7,14,16,18	4,8,9,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,7,18	4,8,9,11,13,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,16,17	4,8,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,7	4,8,9,11,13,15	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,16,17,18	4,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,7,14,17	4,8,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,7,14,16,18	4,8,9,11,13,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,7,14,17,18	4,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,7,14,16	4,8,9,11,13,15	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,7,12,17,18	4,8,9,11,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,7,12,16	4,8,9,11	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,7,12,17	4,8,9,11,15,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,7,12,16,18	4,8,9,11,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,7,12,14	4,8,9,11	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,7,12,14,16,17,18	4,8,9,11,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,7,12,14,18	4,8,9,11,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,7,12,14,16,17	4,8,9,11,15,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,7,12,17	4,8,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,7,12,16,18	4,8,9,11,13,18	2^{-1}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,7,12,17,18	4,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,7,12,16	4,8,9,11,13,15	2^{-1}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,7,12,14,18	4,8,9,11,13,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,7,12,14,16,17	4,8,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,7,12,14	4,8,9,11,13,15	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,7,12,14,16,17,18	4,8,9,11,13,15,17,18	$2^{-17.5}$

Table 0.1503 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,7,10,17	4,8,9,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,7,10,16,18	4,8,9,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,7,10,17,18	4,8,9,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,7,10,16	4,8,9,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,7,10,14,18	4,8,9,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,7,10,14,16,17	4,8,9,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,7,10,14	4,8,9,15	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,7,10,14,16,17,18	4,8,9,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,7,10,17,18	4,8,9,13,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,7,10,16	4,8,9,13	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,7,10,17	4,8,9,13,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,7,10,16,18	4,8,9,13,15,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,7,10,14	4,8,9,13	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,7,10,14,16,17,18	4,8,9,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,7,10,14,18	4,8,9,13,15,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,7,10,14,16,17	4,8,9,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,7,10,12,18	4,8,9,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,7,10,12,16,17	4,8,9,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,7,10,12	4,8,9,15	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,7,10,12,16,17,18	4,8,9,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,7,10,12,14,17	4,8,9,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,7,10,12,14,16,18	4,8,9,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,7,10,12,14,17,18	4,8,9,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,7,10,12,14,16	4,8,9,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,7,10,12	4,8,9,13	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,7,10,12,16,17,18	4,8,9,13,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,7,10,12,18	4,8,9,13,15,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,7,10,12,16,17	4,8,9,13,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,7,10,12,14,17,18	4,8,9,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,7,10,12,14,16	4,8,9,13	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,7,10,12,14,17	4,8,9,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,7,10,12,14,16,18	4,8,9,13,15,18	2^{-23}

Table 0.1504 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,7,10,17,18	4,8,9,11,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,7,10,16	4,8,9,11	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,7,10,17	4,8,9,11,15,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,7,10,16,18	4,8,9,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,7,10,14	4,8,9,11	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,7,10,14,16,17,18	4,8,9,11,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7,10,14,18	4,8,9,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,7,10,14,16,17	4,8,9,11,15,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,7,10,17	4,8,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,7,10,16,18	4,8,9,11,13,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,7,10,17,18	4,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,7,10,16	4,8,9,11,13,15	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,7,10,14,18	4,8,9,11,13,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,7,10,14,16,17	4,8,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,7,10,14	4,8,9,11,13,15	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,7,10,14,16,17,18	4,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,7,10,12	4,8,9,11	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,7,10,12,16,17,18	4,8,9,11,17,18	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,7,10,12,18	4,8,9,11,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,7,10,12,16,17	4,8,9,11,15,17	2^{-12}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,7,10,12,14,17,18	4,8,9,11,17,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,7,10,12,14,16	4,8,9,11	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,7,10,12,14,17	4,8,9,11,15,17	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,7,10,12,14,16,18	4,8,9,11,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7,10,12,18	4,8,9,11,13,18	2^{-34}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,7,10,12,16,17	4,8,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7,10,12	4,8,9,11,13,15	2^{-34}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,7,10,12,16,17,18	4,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,7,10,12,14,17	4,8,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,7,10,12,14,16,18	4,8,9,11,13,18	2^{-23}
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,7,10,12,14,17,18	4,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,7,10,12,14,16	4,8,9,11,13,15	2^{-23}

Table 0.1505 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,18	4,6,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,16,17	4,6,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,5	4,6,15	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,16,17,18	4,6,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,14,17	4,6,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,14,16,18	4,6,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,14,17,18	4,6,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,14,16	4,6,15	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,5	4,6,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,16,17,18	4,6,13,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,18	4,6,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,16,17	4,6,13,15,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,14,17,18	4,6,13,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,14,16	4,6,13	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,14,17	4,6,13,15,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,14,16,18	4,6,13,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,12,17	4,6,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,12,16,18	4,6,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,12,17,18	4,6,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,12,16	4,6,15	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,12,14,18	4,6,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,12,14,16,17	4,6,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,12,14	4,6,15	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,12,14,16,17,18	4,6,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,12,17,18	4,6,13,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,12,16	4,6,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,12,17	4,6,13,15,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,12,16,18	4,6,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,12,14	4,6,13	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,12,14,16,17,18	4,6,13,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,12,14,18	4,6,13,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,12,14,16,17	4,6,13,15,17	2^{-23}

Table 0.1506 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,5	4,6,11	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,16,17,18	4,6,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,18	4,6,11,15,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,16,17	4,6,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,14,17,18	4,6,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,14,16	4,6,11	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,14,17	4,6,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,14,16,18	4,6,11,15,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,18	4,6,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,16,17	4,6,11,13,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,5	4,6,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,16,17,18	4,6,11,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,14,17	4,6,11,13,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,14,16,18	4,6,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,14,17,18	4,6,11,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,14,16	4,6,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,12,17,18	4,6,11,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,12,16	4,6,11	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,12,17	4,6,11,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,12,16,18	4,6,11,15,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,12,14	4,6,11	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,12,14,16,17,18	4,6,11,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,12,14,18	4,6,11,15,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,12,14,16,17	4,6,11,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,12,17	4,6,11,13,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,12,16,18	4,6,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,12,17,18	4,6,11,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,12,16	4,6,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,12,14,18	4,6,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,12,14,16,17	4,6,11,13,17	2^{-34}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,12,14	4,6,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,12,14,16,17,18	4,6,11,13,15,17,18	2^{-34}

Table 0.1507 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,10,17	4,6,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,10,16,18	4,6,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,10,17,18	4,6,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,10,16	4,6,15	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,10,14,18	4,6,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,10,14,16,17	4,6,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,10,14	4,6,15	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,10,14,16,17,18	4,6,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,10,17,18	4,6,13,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,10,16	4,6,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,10,17	4,6,13,15,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,10,16,18	4,6,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,10,14	4,6,13	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,10,14,16,17,18	4,6,13,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,10,14,18	4,6,13,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,10,14,16,17	4,6,13,15,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,10,12,18	4,6,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,10,12,16,17	4,6,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,10,12	4,6,15	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,10,12,16,17,18	4,6,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,10,12,14,17	4,6,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,10,12,14,16,18	4,6,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,10,12,14,17,18	4,6,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,10,12,14,16	4,6,15	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,10,12	4,6,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,10,12,16,17,18	4,6,13,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,10,12,18	4,6,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,10,12,16,17	4,6,13,15,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,10,12,14,17,18	4,6,13,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,10,12,14,16	4,6,13	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,10,12,14,17	4,6,13,15,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,10,12,14,16,18	4,6,13,15,18	$2^{-28.5}$

Table 0.1508 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,10,17,18	4,6,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,10,16	4,6,11	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,10,17	4,6,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,10,16,18	4,6,11,15,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,10,14	4,6,11	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,10,14,16,17,18	4,6,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,10,14,18	4,6,11,15,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,10,14,16,17	4,6,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,10,17	4,6,11,13,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,10,16,18	4,6,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,10,17,18	4,6,11,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,10,16	4,6,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,10,14,18	4,6,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,10,14,16,17	4,6,11,13,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,10,14	4,6,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,10,14,16,17,18	4,6,11,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,10,12	4,6,11	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,10,12,16,17,18	4,6,11,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,10,12,18	4,6,11,15,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,10,12,16,17	4,6,11,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,10,12,14,17,18	4,6,11,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,10,12,14,16	4,6,11	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,10,12,14,17	4,6,11,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,10,12,14,16,18	4,6,11,15,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,10,12,18	4,6,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,10,12,16,17	4,6,11,13,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,10,12	4,6,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,10,12,16,17,18	4,6,11,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,10,12,14,17	4,6,11,13,17	2^{-1}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,10,12,14,16,18	4,6,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,10,12,14,17,18	4,6,11,13,15,17,18	2^{-1}
$(1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,10,12,14,16	4,6,11,13,15	$2^{-17.5}$

Table 0.1509 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,5	4,6,9	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,16,17,18	4,6,9,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,18	4,6,9,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,16,17	4,6,9,15,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,14,17,18	4,6,9,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,14,16	4,6,9	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,14,17	4,6,9,15,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,14,16,18	4,6,9,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,18	4,6,9,13,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,16,17	4,6,9,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,5	4,6,9,13,15	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,16,17,18	4,6,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,14,17	4,6,9,13,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,14,16,18	4,6,9,13,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,14,17,18	4,6,9,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,14,16	4,6,9,13,15	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,12,17,18	4,6,9,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,12,16	4,6,9	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,12,17	4,6,9,15,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,12,16,18	4,6,9,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,12,14	4,6,9	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,12,14,16,17,18	4,6,9,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,12,14,18	4,6,9,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,12,14,16,17	4,6,9,15,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,12,17	4,6,9,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,12,16,18	4,6,9,13,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,12,17,18	4,6,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,12,16	4,6,9,13,15	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,12,14,18	4,6,9,13,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,12,14,16,17	4,6,9,13,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,12,14	4,6,9,13,15	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,12,14,16,17,18	4,6,9,13,15,17,18	$2^{-28.5}$

Table 0.1510 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,18	4,6,9,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,16,17	4,6,9,11,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5	4,6,9,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,16,17,18	4,6,9,11,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,14,17	4,6,9,11,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,14,16,18	4,6,9,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,14,17,18	4,6,9,11,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,14,16	4,6,9,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,5	4,6,9,11,13	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,16,17,18	4,6,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,18	4,6,9,11,13,15,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,16,17	4,6,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,14,17,18	4,6,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,14,16	4,6,9,11,13	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,14,17	4,6,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,14,16,18	4,6,9,11,13,15,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,12,17	4,6,9,11,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,12,16,18	4,6,9,11,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,12,17,18	4,6,9,11,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,12,16	4,6,9,11,15	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,12,14,18	4,6,9,11,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,12,14,16,17	4,6,9,11,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,12,14	4,6,9,11,15	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,12,14,16,17,18	4,6,9,11,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,12,17,18	4,6,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,12,16	4,6,9,11,13	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,12,17	4,6,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,12,16,18	4,6,9,11,13,15,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,12,14	4,6,9,11,13	2^{-1}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,12,14,16,17,18	4,6,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,12,14,18	4,6,9,11,13,15,18	2^{-1}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,12,14,16,17	4,6,9,11,13,15,17	$2^{-17.5}$

Table 0.1511 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,10,17,18	4,6,9,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,10,16	4,6,9	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,10,17	4,6,9,15,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,10,16,18	4,6,9,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,10,14	4,6,9	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,10,14,16,17,18	4,6,9,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,10,14,18	4,6,9,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,10,14,16,17	4,6,9,15,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,10,17	4,6,9,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,10,16,18	4,6,9,13,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,10,17,18	4,6,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,10,16	4,6,9,13,15	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,10,14,18	4,6,9,13,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,10,14,16,17	4,6,9,13,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,10,14	4,6,9,13,15	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,10,14,16,17,18	4,6,9,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,10,12	4,6,9	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,10,12,16,17,18	4,6,9,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,10,12,18	4,6,9,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,10,12,16,17	4,6,9,15,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,10,12,14,17,18	4,6,9,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,10,12,14,16	4,6,9	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,10,12,14,17	4,6,9,15,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,10,12,14,16,18	4,6,9,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,10,12,18	4,6,9,13,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,10,12,16,17	4,6,9,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,10,12	4,6,9,13,15	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,10,12,16,17,18	4,6,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,10,12,14,17	4,6,9,13,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,10,12,14,16,18	4,6,9,13,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,10,12,14,17,18	4,6,9,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,10,12,14,16	4,6,9,13,15	2^{-23}

Table 0.1512 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,10,17	4,6,9,11,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,10,16,18	4,6,9,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,10,17,18	4,6,9,11,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,10,16	4,6,9,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,10,14,18	4,6,9,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,10,14,16,17	4,6,9,11,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,10,14	4,6,9,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,10,14,16,17,18	4,6,9,11,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,10,17,18	4,6,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,10,16	4,6,9,11,13	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,10,17	4,6,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,10,16,18	4,6,9,11,13,15,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,10,14	4,6,9,11,13	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,10,14,16,17,18	4,6,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,10,14,18	4,6,9,11,13,15,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,10,14,16,17	4,6,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,10,12,18	4,6,9,11,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,10,12,16,17	4,6,9,11,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,10,12	4,6,9,11,15	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,10,12,16,17,18	4,6,9,11,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,10,12,14,17	4,6,9,11,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,10,12,14,16,18	4,6,9,11,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,10,12,14,17,18	4,6,9,11,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,10,12,14,16	4,6,9,11,15	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,10,12	4,6,9,11,13	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,10,12,16,17,18	4,6,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,10,12,18	4,6,9,11,13,15,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,10,12,16,17	4,6,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,10,12,14,17,18	4,6,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,10,12,14,16	4,6,9,11,13	2^{-34}
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,10,12,14,17	4,6,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,10,12,14,16,18	4,6,9,11,13,15,18	2^{-34}

Table 0.1513 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,17	4,6,8,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,16,18	4,6,8,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,17,18	4,6,8,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,16	4,6,8,15	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,14,18	4,6,8,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,14,16,17	4,6,8,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,14	4,6,8,15	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,14,16,17,18	4,6,8,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,17,18	4,6,8,13,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,16	4,6,8,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,17	4,6,8,13,15,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,16,18	4,6,8,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,14	4,6,8,13	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,14,16,17,18	4,6,8,13,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,14,18	4,6,8,13,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,14,16,17	4,6,8,13,15,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,12,18	4,6,8,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,12,16,17	4,6,8,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,12	4,6,8,15	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,12,16,17,18	4,6,8,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,12,14,17	4,6,8,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,12,14,16,18	4,6,8,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,12,14,17,18	4,6,8,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,12,14,16	4,6,8,15	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,12	4,6,8,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,12,16,17,18	4,6,8,13,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,12,18	4,6,8,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,12,16,17	4,6,8,13,15,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,12,14,17,18	4,6,8,13,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,12,14,16	4,6,8,13	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,12,14,17	4,6,8,13,15,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,12,14,16,18	4,6,8,13,15,18	$2^{-6.5}$

Table 0.1514 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,17,18	4,6,8,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,16	4,6,8,11	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,17	4,6,8,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,16,18	4,6,8,11,15,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,14	4,6,8,11	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,14,16,17,18	4,6,8,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,14,18	4,6,8,11,15,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,14,16,17	4,6,8,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,17	4,6,8,11,13,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,16,18	4,6,8,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,17,18	4,6,8,11,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,16	4,6,8,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,14,18	4,6,8,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,14,16,17	4,6,8,11,13,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,14	4,6,8,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,14,16,17,18	4,6,8,11,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,12	4,6,8,11	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,12,16,17,18	4,6,8,11,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,12,18	4,6,8,11,15,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,12,16,17	4,6,8,11,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,12,14,17,18	4,6,8,11,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,12,14,16	4,6,8,11	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,12,14,17	4,6,8,11,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,12,14,16,18	4,6,8,11,15,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,12,18	4,6,8,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,12,16,17	4,6,8,11,13,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,12	4,6,8,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,12,16,17,18	4,6,8,11,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,12,14,17	4,6,8,11,13,17	2^{-34}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,12,14,16,18	4,6,8,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,12,14,17,18	4,6,8,11,13,15,17,18	2^{-34}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,12,14,16	4,6,8,11,13,15	$2^{-17.5}$

Table 0.1515 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,10,18	4,6,8,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,10,16,17	4,6,8,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,10	4,6,8,15	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,10,16,17,18	4,6,8,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,10,14,17	4,6,8,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,10,14,16,18	4,6,8,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,10,14,17,18	4,6,8,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,10,14,16	4,6,8,15	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,10	4,6,8,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,10,16,17,18	4,6,8,13,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,10,18	4,6,8,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,10,16,17	4,6,8,13,15,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,10,14,17,18	4,6,8,13,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,10,14,16	4,6,8,13	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,10,14,17	4,6,8,13,15,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,10,14,16,18	4,6,8,13,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,10,12,17	4,6,8,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,10,12,16,18	4,6,8,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,10,12,17,18	4,6,8,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,10,12,16	4,6,8,15	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,10,12,14,18	4,6,8,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,10,12,14,16,17	4,6,8,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,10,12,14	4,6,8,15	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,10,12,14,16,17,18	4,6,8,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,10,12,17,18	4,6,8,13,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,10,12,16	4,6,8,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,10,12,17	4,6,8,13,15,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,10,12,16,18	4,6,8,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,10,12,14	4,6,8,13	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,10,12,14,16,17,18	4,6,8,13,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,10,12,14,18	4,6,8,13,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,10,12,14,16,17	4,6,8,13,15,17	2^{-12}

Table 0.1516 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,10	4,6,8,11	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,10,16,17,18	4,6,8,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,10,18	4,6,8,11,15,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,10,16,17	4,6,8,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,10,14,17,18	4,6,8,11,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,10,14,16	4,6,8,11	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,10,14,17	4,6,8,11,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,10,14,16,18	4,6,8,11,15,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,10,18	4,6,8,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,10,16,17	4,6,8,11,13,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,10	4,6,8,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,10,16,17,18	4,6,8,11,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,10,14,17	4,6,8,11,13,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,10,14,16,18	4,6,8,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,10,14,17,18	4,6,8,11,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,10,14,16	4,6,8,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,10,12,17,18	4,6,8,11,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,10,12,16	4,6,8,11	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,10,12,17	4,6,8,11,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,10,12,16,18	4,6,8,11,15,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,10,12,14	4,6,8,11	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,10,12,14,16,17,18	4,6,8,11,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,10,12,14,18	4,6,8,11,15,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,10,12,14,16,17	4,6,8,11,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,10,12,17	4,6,8,11,13,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,10,12,16,18	4,6,8,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,10,12,17,18	4,6,8,11,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,10,12,16	4,6,8,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,10,12,14,18	4,6,8,11,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,10,12,14,16,17	4,6,8,11,13,17	2^{-1}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,10,12,14	4,6,8,11,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,10,12,14,16,17,18	4,6,8,11,13,15,17,18	2^{-1}

Table 0.1517 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,17,18	4,6,8,9,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,16	4,6,8,9	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,17	4,6,8,9,15,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,16,18	4,6,8,9,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,14	4,6,8,9	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,14,16,17,18	4,6,8,9,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,14,18	4,6,8,9,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,14,16,17	4,6,8,9,15,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,17	4,6,8,9,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,16,18	4,6,8,9,13,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,17,18	4,6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,16	4,6,8,9,13,15	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,14,18	4,6,8,9,13,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,14,16,17	4,6,8,9,13,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,14	4,6,8,9,13,15	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,14,16,17,18	4,6,8,9,13,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,12	4,6,8,9	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,12,16,17,18	4,6,8,9,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,12,18	4,6,8,9,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,12,16,17	4,6,8,9,15,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,12,14,17,18	4,6,8,9,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,12,14,16	4,6,8,9	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,12,14,17	4,6,8,9,15,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,12,14,16,18	4,6,8,9,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,12,18	4,6,8,9,13,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,12,16,17	4,6,8,9,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,12	4,6,8,9,13,15	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,12,16,17,18	4,6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,12,14,17	4,6,8,9,13,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,12,14,16,18	4,6,8,9,13,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,12,14,17,18	4,6,8,9,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,12,14,16	4,6,8,9,13,15	2^{-12}

Table 0.1518 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,17	4,6,8,9,11,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,16,18	4,6,8,9,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,17,18	4,6,8,9,11,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,16	4,6,8,9,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,14,18	4,6,8,9,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,14,16,17	4,6,8,9,11,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,14	4,6,8,9,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,14,16,17,18	4,6,8,9,11,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,17,18	4,6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,16	4,6,8,9,11,13	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,17	4,6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,16,18	4,6,8,9,11,13,15,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,14	4,6,8,9,11,13	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,14,16,17,18	4,6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,14,18	4,6,8,9,11,13,15,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,14,16,17	4,6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,12,18	4,6,8,9,11,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,12,16,17	4,6,8,9,11,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,12	4,6,8,9,11,15	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,12,16,17,18	4,6,8,9,11,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,12,14,17	4,6,8,9,11,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,12,14,16,18	4,6,8,9,11,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,12,14,17,18	4,6,8,9,11,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,12,14,16	4,6,8,9,11,15	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,12	4,6,8,9,11,13	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,12,16,17,18	4,6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,12,18	4,6,8,9,11,13,15,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,12,16,17	4,6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,12,14,17,18	4,6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,12,14,16	4,6,8,9,11,13	2^{-1}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,12,14,17	4,6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,12,14,16,18	4,6,8,9,11,13,15,18	2^{-1}

Table 0.1519 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,10	4,6,8,9	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,10,16,17,18	4,6,8,9,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,10,18	4,6,8,9,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,10,16,17	4,6,8,9,15,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,10,14,17,18	4,6,8,9,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,10,14,16	4,6,8,9	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,10,14,17	4,6,8,9,15,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,10,14,16,18	4,6,8,9,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,10,18	4,6,8,9,13,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,10,16,17	4,6,8,9,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,10	4,6,8,9,13,15	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,10,16,17,18	4,6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,10,14,17	4,6,8,9,13,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,10,14,16,18	4,6,8,9,13,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,10,14,17,18	4,6,8,9,13,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,10,14,16	4,6,8,9,13,15	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,10,12,17,18	4,6,8,9,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,10,12,16	4,6,8,9	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,10,12,17	4,6,8,9,15,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,10,12,16,18	4,6,8,9,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,10,12,14	4,6,8,9	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,10,12,14,16,17,18	4,6,8,9,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,10,12,14,18	4,6,8,9,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,10,12,14,16,17	4,6,8,9,15,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,10,12,17	4,6,8,9,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,10,12,16,18	4,6,8,9,13,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,10,12,17,18	4,6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,10,12,16	4,6,8,9,13,15	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,10,12,14,18	4,6,8,9,13,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,10,12,14,16,17	4,6,8,9,13,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,10,12,14	4,6,8,9,13,15	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,10,12,14,16,17,18	4,6,8,9,13,15,17,18	$2^{-6.5}$

Table 0.1520 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,10,18	4,6,8,9,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,10,16,17	4,6,8,9,11,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,10	4,6,8,9,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,10,16,17,18	4,6,8,9,11,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,10,14,17	4,6,8,9,11,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,10,14,16,18	4,6,8,9,11,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,10,14,17,18	4,6,8,9,11,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,10,14,16	4,6,8,9,11,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,10	4,6,8,9,11,13	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,10,16,17,18	4,6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,10,18	4,6,8,9,11,13,15,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,10,16,17	4,6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,10,14,17,18	4,6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,10,14,16	4,6,8,9,11,13	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,10,14,17	4,6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,10,14,16,18	4,6,8,9,11,13,15,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,10,12,17	4,6,8,9,11,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,10,12,16,18	4,6,8,9,11,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,10,12,17,18	4,6,8,9,11,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,10,12,16	4,6,8,9,11,15	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,10,12,14,18	4,6,8,9,11,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,10,12,14,16,17	4,6,8,9,11,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,10,12,14	4,6,8,9,11,15	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,10,12,14,16,17,18	4,6,8,9,11,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,10,12,17,18	4,6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,10,12,16	4,6,8,9,11,13	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,10,12,17	4,6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,10,12,16,18	4,6,8,9,11,13,15,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,10,12,14	4,6,8,9,11,13	2^{-34}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,10,12,14,16,17,18	4,6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,10,12,14,18	4,6,8,9,11,13,15,18	2^{-34}
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,10,12,14,16,17	4,6,8,9,11,13,15,17	$2^{-17.5}$

Table 0.1521 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,7	4,6	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,7,16,17,18	4,6,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,7,18	4,6,15,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,7,16,17	4,6,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,7,14,17,18	4,6,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,7,14,16	4,6	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,7,14,17	4,6,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,7,14,16,18	4,6,15,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,7,18	4,6,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,7,16,17	4,6,13,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,7	4,6,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,7,16,17,18	4,6,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,7,14,17	4,6,13,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,7,14,16,18	4,6,13,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,7,14,17,18	4,6,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,7,14,16	4,6,13,15	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,7,12,17,18	4,6,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,7,12,16	4,6	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,12,17	4,6,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,7,12,16,18	4,6,15,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,7,12,14	4,6	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,12,14,16,17,18	4,6,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,7,12,14,18	4,6,15,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,12,14,16,17	4,6,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,7,12,17	4,6,13,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,7,12,16,18	4,6,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,7,12,17,18	4,6,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,7,12,16	4,6,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,7,12,14,18	4,6,13,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,7,12,14,16,17	4,6,13,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,7,12,14	4,6,13,15	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,7,12,14,16,17,18	4,6,13,15,17,18	2^{-23}

Table 0.1522 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,7,18	4,6,11,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,7,16,17	4,6,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,7	4,6,11,15	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,7,16,17,18	4,6,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,7,14,17	4,6,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,7,14,16,18	4,6,11,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,7,14,17,18	4,6,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,7,14,16	4,6,11,15	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,7	4,6,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,7,16,17,18	4,6,11,13,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,7,18	4,6,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,7,16,17	4,6,11,13,15,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,7,14,17,18	4,6,11,13,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,7,14,16	4,6,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,7,14,17	4,6,11,13,15,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,7,14,16,18	4,6,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,7,12,17	4,6,11,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,7,12,16,18	4,6,11,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,7,12,17,18	4,6,11,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,7,12,16	4,6,11,15	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,7,12,14,18	4,6,11,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,7,12,14,16,17	4,6,11,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,7,12,14	4,6,11,15	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,7,12,14,16,17,18	4,6,11,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,7,12,17,18	4,6,11,13,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,7,12,16	4,6,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,7,12,17	4,6,11,13,15,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,7,12,16,18	4,6,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,12,14	4,6,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,7,12,14,16,17,18	4,6,11,13,17,18	2^{-34}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,12,14,18	4,6,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,7,12,14,16,17	4,6,11,13,15,17	2^{-34}

Table 0.1523 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,7,10,17,18	4,6,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,7,10,16	4,6	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,7,10,17	4,6,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,7,10,16,18	4,6,15,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,7,10,14	4,6	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,7,10,14,16,17,18	4,6,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,7,10,14,18	4,6,15,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,7,10,14,16,17	4,6,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,7,10,17	4,6,13,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,7,10,16,18	4,6,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,7,10,17,18	4,6,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,7,10,16	4,6,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,7,10,14,18	4,6,13,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,7,10,14,16,17	4,6,13,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,7,10,14	4,6,13,15	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,7,10,14,16,17,18	4,6,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,7,10,12	4,6	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,7,10,12,16,17,18	4,6,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,7,10,12,18	4,6,15,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,7,10,12,16,17	4,6,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,7,10,12,14,17,18	4,6,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,7,10,12,14,16	4,6	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,7,10,12,14,17	4,6,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,7,10,12,14,16,18	4,6,15,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,7,10,12,18	4,6,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,7,10,12,16,17	4,6,13,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,7,10,12	4,6,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,7,10,12,16,17,18	4,6,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,7,10,12,14,17	4,6,13,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,7,10,12,14,16,18	4,6,13,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,7,10,12,14,17,18	4,6,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,7,10,12,14,16	4,6,13,15	$2^{-28.5}$

Table 0.1524 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,7,10,17	4,6,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,7,10,16,18	4,6,11,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,7,10,17,18	4,6,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,7,10,16	4,6,11,15	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,7,10,14,18	4,6,11,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,7,10,14,16,17	4,6,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,7,10,14	4,6,11,15	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,7,10,14,16,17,18	4,6,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,7,10,17,18	4,6,11,13,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,7,10,16	4,6,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,7,10,17	4,6,11,13,15,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,7,10,16,18	4,6,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,7,10,14	4,6,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7,10,14,16,17,18	4,6,11,13,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,7,10,14,18	4,6,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7,10,14,16,17	4,6,11,13,15,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,7,10,12,18	4,6,11,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,7,10,12,16,17	4,6,11,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,7,10,12	4,6,11,15	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,7,10,12,16,17,18	4,6,11,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,7,10,12,14,17	4,6,11,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,7,10,12,14,16,18	4,6,11,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,7,10,12,14,17,18	4,6,11,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,7,10,12,14,16	4,6,11,15	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,7,10,12	4,6,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,7,10,12,16,17,18	4,6,11,13,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,7,10,12,18	4,6,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,7,10,12,16,17	4,6,11,13,15,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,7,10,12,14,17,18	4,6,11,13,17,18	2^{-1}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,7,10,12,14,16	4,6,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,7,10,12,14,17	4,6,11,13,15,17	2^{-1}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,7,10,12,14,16,18	4,6,11,13,15,18	$2^{-17.5}$

Table 0.1525 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,7,18	4,6,9,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,7,16,17	4,6,9,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,7	4,6,9,15	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,7,16,17,18	4,6,9,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,7,14,17	4,6,9,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,7,14,16,18	4,6,9,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,7,14,17,18	4,6,9,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,7,14,16	4,6,9,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,7	4,6,9,13	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,7,16,17,18	4,6,9,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,7,18	4,6,9,13,15,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,7,16,17	4,6,9,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,7,14,17,18	4,6,9,13,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,7,14,16	4,6,9,13	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,7,14,17	4,6,9,13,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,7,14,16,18	4,6,9,13,15,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,7,12,17	4,6,9,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,7,12,16,18	4,6,9,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,7,12,17,18	4,6,9,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,7,12,16	4,6,9,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,7,12,14,18	4,6,9,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,7,12,14,16,17	4,6,9,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,7,12,14	4,6,9,15	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,7,12,14,16,17,18	4,6,9,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,7,12,17,18	4,6,9,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,7,12,16	4,6,9,13	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,7,12,17	4,6,9,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,7,12,16,18	4,6,9,13,15,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,7,12,14	4,6,9,13	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,7,12,14,16,17,18	4,6,9,13,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,7,12,14,18	4,6,9,13,15,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,7,12,14,16,17	4,6,9,13,15,17	$2^{-28.5}$

Table 0.1526 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,7	4,6,9,11	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,7,16,17,18	4,6,9,11,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,7,18	4,6,9,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,7,16,17	4,6,9,11,15,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,7,14,17,18	4,6,9,11,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,7,14,16	4,6,9,11	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,7,14,17	4,6,9,11,15,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,7,14,16,18	4,6,9,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,7,18	4,6,9,11,13,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,7,16,17	4,6,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,7	4,6,9,11,13,15	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,7,16,17,18	4,6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,7,14,17	4,6,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,7,14,16,18	4,6,9,11,13,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,7,14,17,18	4,6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,7,14,16	4,6,9,11,13,15	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,7,12,17,18	4,6,9,11,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,7,12,16	4,6,9,11	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,7,12,17	4,6,9,11,15,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,7,12,16,18	4,6,9,11,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,7,12,14	4,6,9,11	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,7,12,14,16,17,18	4,6,9,11,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,7,12,14,18	4,6,9,11,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,7,12,14,16,17	4,6,9,11,15,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,7,12,17	4,6,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,7,12,16,18	4,6,9,11,13,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,7,12,17,18	4,6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,7,12,16	4,6,9,11,13,15	2^{-12}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,7,12,14,18	4,6,9,11,13,18	2^{-1}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,7,12,14,16,17	4,6,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,7,12,14	4,6,9,11,13,15	2^{-1}
$(1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,7,12,14,16,17,18	4,6,9,11,13,15,17,18	$2^{-17.5}$

Table 0.1527 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,7,10,17	4,6,9,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,7,10,16,18	4,6,9,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,7,10,17,18	4,6,9,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,7,10,16	4,6,9,15	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10,14,18	4,6,9,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,14,16,17	4,6,9,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10,14	4,6,9,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,14,16,17,18	4,6,9,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,7,10,17,18	4,6,9,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,7,10,16	4,6,9,13	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,7,10,17	4,6,9,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,7,10,16,18	4,6,9,13,15,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10,14	4,6,9,13	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,7,10,14,16,17,18	4,6,9,13,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10,14,18	4,6,9,13,15,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,14,16,17	4,6,9,13,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,7,10,12,18	4,6,9,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,7,10,12,16,17	4,6,9,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,7,10,12	4,6,9,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,7,10,12,16,17,18	4,6,9,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,7,10,12,14,17	4,6,9,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,7,10,12,14,16,18	4,6,9,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,7,10,12,14,17,18	4,6,9,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,7,10,12,14,16	4,6,9,15	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,7,10,12	4,6,9,13	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,7,10,12,16,17,18	4,6,9,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,7,10,12,18	4,6,9,13,15,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,7,10,12,16,17	4,6,9,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,7,10,12,14,17,18	4,6,9,13,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,7,10,12,14,16	4,6,9,13	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,7,10,12,14,17	4,6,9,13,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,7,10,12,14,16,18	4,6,9,13,15,18	2^{-23}

Table 0.1528 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,7,10,17,18	4,6,9,11,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,7,10,16	4,6,9,11	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,7,10,17	4,6,9,11,15,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,7,10,16,18	4,6,9,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,7,10,14	4,6,9,11	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7,10,14,16,17,18	4,6,9,11,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,7,10,14,18	4,6,9,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7,10,14,16,17	4,6,9,11,15,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,7,10,17	4,6,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,7,10,16,18	4,6,9,11,13,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,7,10,17,18	4,6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,7,10,16	4,6,9,11,13,15	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,7,10,14,18	4,6,9,11,13,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,7,10,14,16,17	4,6,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,7,10,14	4,6,9,11,13,15	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,7,10,14,16,17,18	4,6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,7,10,12	4,6,9,11	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,7,10,12,16,17,18	4,6,9,11,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,7,10,12,18	4,6,9,11,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,7,10,12,16,17	4,6,9,11,15,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,7,10,12,14,17,18	4,6,9,11,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,7,10,12,14,16	4,6,9,11	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,7,10,12,14,17	4,6,9,11,15,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7,10,12,14,16,18	4,6,9,11,15,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,7,10,12,18	4,6,9,11,13,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,7,10,12,16,17	4,6,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,7,10,12	4,6,9,11,13,15	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,7,10,12,16,17,18	4,6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,7,10,12,14,17	4,6,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,7,10,12,14,16,18	4,6,9,11,13,18	2^{-34}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,7,10,12,14,17,18	4,6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,7,10,12,14,16	4,6,9,11,13,15	2^{-34}

Table 0.1529 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,7,17,18	4,6,8,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,7,16	4,6,8	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,7,17	4,6,8,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,7,16,18	4,6,8,15,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,7,14	4,6,8	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,7,14,16,17,18	4,6,8,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,7,14,18	4,6,8,15,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,7,14,16,17	4,6,8,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,7,17	4,6,8,13,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,7,16,18	4,6,8,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,7,17,18	4,6,8,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,7,16	4,6,8,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,7,14,18	4,6,8,13,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,7,14,16,17	4,6,8,13,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,7,14	4,6,8,13,15	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,7,14,16,17,18	4,6,8,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,7,12	4,6,8	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,7,12,16,17,18	4,6,8,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,7,12,18	4,6,8,15,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,7,12,16,17	4,6,8,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,7,12,14,17,18	4,6,8,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,7,12,14,16	4,6,8	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,7,12,14,17	4,6,8,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,7,12,14,16,18	4,6,8,15,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,7,12,18	4,6,8,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,7,12,16,17	4,6,8,13,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,7,12	4,6,8,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,7,12,16,17,18	4,6,8,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,7,12,14,17	4,6,8,13,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,7,12,14,16,18	4,6,8,13,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,7,12,14,17,18	4,6,8,13,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,7,12,14,16	4,6,8,13,15	$2^{-6.5}$

Table 0.1530 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,7,17	4,6,8,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,7,16,18	4,6,8,11,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,7,17,18	4,6,8,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,7,16	4,6,8,11,15	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7,14,18	4,6,8,11,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,7,14,16,17	4,6,8,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7,14	4,6,8,11,15	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,7,14,16,17,18	4,6,8,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,7,17,18	4,6,8,11,13,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,7,16	4,6,8,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,7,17	4,6,8,11,13,15,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,7,16,18	4,6,8,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,7,14	4,6,8,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,7,14,16,17,18	4,6,8,11,13,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,7,14,18	4,6,8,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,7,14,16,17	4,6,8,11,13,15,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,7,12,18	4,6,8,11,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,7,12,16,17	4,6,8,11,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,7,12	4,6,8,11,15	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,7,12,16,17,18	4,6,8,11,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,7,12,14,17	4,6,8,11,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,7,12,14,16,18	4,6,8,11,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,7,12,14,17,18	4,6,8,11,15,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,7,12,14,16	4,6,8,11,15	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,7,12	4,6,8,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,7,12,16,17,18	4,6,8,11,13,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,7,12,18	4,6,8,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,7,12,16,17	4,6,8,11,13,15,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,7,12,14,17,18	4,6,8,11,13,17,18	2^{-34}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,7,12,14,16	4,6,8,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,7,12,14,17	4,6,8,11,13,15,17	2^{-34}
$(1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,7,12,14,16,18	4,6,8,11,13,15,18	$2^{-17.5}$

Table 0.1531 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10	4,6,8	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,16,17,18	4,6,8,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10,18	4,6,8,15,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,16,17	4,6,8,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,14,17,18	4,6,8,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,7,10,14,16	4,6,8	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,14,17	4,6,8,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,7,10,14,16,18	4,6,8,15,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,7,10,18	4,6,8,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,16,17	4,6,8,13,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10	4,6,8,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,16,17,18	4,6,8,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,14,17	4,6,8,13,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,7,10,14,16,18	4,6,8,13,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,14,17,18	4,6,8,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,7,10,14,16	4,6,8,13,15	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,12,17,18	4,6,8,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,7,10,12,16	4,6,8	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,7,10,12,17	4,6,8,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,7,10,12,16,18	4,6,8,15,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10,12,14	4,6,8	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,12,14,16,17,18	4,6,8,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10,12,14,18	4,6,8,15,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,12,14,16,17	4,6,8,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,12,17	4,6,8,13,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,7,10,12,16,18	4,6,8,13,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,7,10,12,17,18	4,6,8,13,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,7,10,12,16	4,6,8,13,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10,12,14,18	4,6,8,13,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,12,14,16,17	4,6,8,13,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,7,10,12,14	4,6,8,13,15	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,12,14,16,17,18	4,6,8,13,15,17,18	2^{-12}

Table 0.1532 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,7,10,18	4,6,8,11,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,7,10,16,17	4,6,8,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,7,10	4,6,8,11,15	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,7,10,16,17,18	4,6,8,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,7,10,14,17	4,6,8,11,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,7,10,14,16,18	4,6,8,11,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,7,10,14,17,18	4,6,8,11,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,7,10,14,16	4,6,8,11,15	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,7,10	4,6,8,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,7,10,16,17,18	4,6,8,11,13,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,7,10,18	4,6,8,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,7,10,16,17	4,6,8,11,13,15,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,7,10,14,17,18	4,6,8,11,13,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,7,10,14,16	4,6,8,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,7,10,14,17	4,6,8,11,13,15,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,7,10,14,16,18	4,6,8,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,7,10,12,17	4,6,8,11,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,7,10,12,16,18	4,6,8,11,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,7,10,12,17,18	4,6,8,11,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,7,10,12,16	4,6,8,11,15	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,7,10,12,14,18	4,6,8,11,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,7,10,12,14,16,17	4,6,8,11,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,7,10,12,14	4,6,8,11,15	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,7,10,12,14,16,17,18	4,6,8,11,15,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,7,10,12,17,18	4,6,8,11,13,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,7,10,12,16	4,6,8,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,7,10,12,17	4,6,8,11,13,15,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,7,10,12,16,18	4,6,8,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,7,10,12,14	4,6,8,11,13	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,7,10,12,14,16,17,18	4,6,8,11,13,17,18	2^{-1}
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,7,10,12,14,18	4,6,8,11,13,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,7,10,12,14,16,17	4,6,8,11,13,15,17	2^{-1}

Table 0.1533 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,7,17	4,6,8,9,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,7,16,18	4,6,8,9,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,7,17,18	4,6,8,9,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,7,16	4,6,8,9,15	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,7,14,18	4,6,8,9,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,7,14,16,17	4,6,8,9,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,7,14	4,6,8,9,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,7,14,16,17,18	4,6,8,9,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,7,17,18	4,6,8,9,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,7,16	4,6,8,9,13	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,7,17	4,6,8,9,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,7,16,18	4,6,8,9,13,15,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,7,14	4,6,8,9,13	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,7,14,16,17,18	4,6,8,9,13,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,7,14,18	4,6,8,9,13,15,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,7,14,16,17	4,6,8,9,13,15,17	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,7,12,18	4,6,8,9,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,7,12,16,17	4,6,8,9,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,7,12	4,6,8,9,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,7,12,16,17,18	4,6,8,9,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,7,12,14,17	4,6,8,9,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,7,12,14,16,18	4,6,8,9,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,7,12,14,17,18	4,6,8,9,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,7,12,14,16	4,6,8,9,15	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,7,12	4,6,8,9,13	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,7,12,16,17,18	4,6,8,9,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,7,12,18	4,6,8,9,13,15,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,7,12,16,17	4,6,8,9,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,7,12,14,17,18	4,6,8,9,13,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,7,12,14,16	4,6,8,9,13	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,7,12,14,17	4,6,8,9,13,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,7,12,14,16,18	4,6,8,9,13,15,18	2^{-12}

Table 0.1534 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,7,17,18	4,6,8,9,11,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,7,16	4,6,8,9,11	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,7,17	4,6,8,9,11,15,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,7,16,18	4,6,8,9,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,7,14	4,6,8,9,11	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,7,14,16,17,18	4,6,8,9,11,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,7,14,18	4,6,8,9,11,15,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,7,14,16,17	4,6,8,9,11,15,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,7,17	4,6,8,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,7,16,18	4,6,8,9,11,13,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,7,17,18	4,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,7,16	4,6,8,9,11,13,15	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7,14,18	4,6,8,9,11,13,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,7,14,16,17	4,6,8,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,7,14	4,6,8,9,11,13,15	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,7,14,16,17,18	4,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,7,12	4,6,8,9,11	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,7,12,16,17,18	4,6,8,9,11,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,7,12,18	4,6,8,9,11,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,7,12,16,17	4,6,8,9,11,15,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,7,12,14,17,18	4,6,8,9,11,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,7,12,14,16	4,6,8,9,11	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,7,12,14,17	4,6,8,9,11,15,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,7,12,14,16,18	4,6,8,9,11,15,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,7,12,18	4,6,8,9,11,13,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,7,12,16,17	4,6,8,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,7,12	4,6,8,9,11,13,15	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,7,12,16,17,18	4,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,7,12,14,17	4,6,8,9,11,13,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,7,12,14,16,18	4,6,8,9,11,13,18	2^{-1}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,7,12,14,17,18	4,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,7,12,14,16	4,6,8,9,11,13,15	2^{-1}

Table 0.1535 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,7,10,18	4,6,8,9,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,16,17	4,6,8,9,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,7,10	4,6,8,9,15	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,16,17,18	4,6,8,9,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,7,10,14,17	4,6,8,9,17	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,7,10,14,16,18	4,6,8,9,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,7,10,14,17,18	4,6,8,9,15,17,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,7,10,14,16	4,6,8,9,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,7,10	4,6,8,9,13	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,16,17,18	4,6,8,9,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,7,10,18	4,6,8,9,13,15,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,16,17	4,6,8,9,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,7,10,14,17,18	4,6,8,9,13,17,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,7,10,14,16	4,6,8,9,13	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,7,10,14,17	4,6,8,9,13,15,17	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,7,10,14,16,18	4,6,8,9,13,15,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,7,10,12,17	4,6,8,9,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,10,12,16,18	4,6,8,9,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,7,10,12,17,18	4,6,8,9,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,10,12,16	4,6,8,9,15	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,10,12,14,18	4,6,8,9,18	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,7,10,12,14,16,17	4,6,8,9,17	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,10,12,14	4,6,8,9,15	$2^{-28.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,7,10,12,14,16,17,18	4,6,8,9,15,17,18	2^{-12}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,7,10,12,17,18	4,6,8,9,13,17,18	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,7,10,12,16	4,6,8,9,13	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,7,10,12,17	4,6,8,9,13,15,17	$2^{-17.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,7,10,12,16,18	4,6,8,9,13,15,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,7,10,12,14	4,6,8,9,13	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,7,10,12,14,16,17,18	4,6,8,9,13,17,18	$2^{-6.5}$
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,7,10,12,14,18	4,6,8,9,13,15,18	2^{-23}
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,7,10,12,14,16,17	4,6,8,9,13,15,17	$2^{-6.5}$

Table 0.1536 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		P
	j values (i odd)	j values (i even)	
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,7,10	4,6,8,9,11	2 ⁻
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,7,10,16,17,18	4,6,8,9,11,17,18	2 ⁻
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,7,10,18	4,6,8,9,11,15,18	2 ⁻
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,7,10,16,17	4,6,8,9,11,15,17	2 ⁻
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,7,10,14,17,18	4,6,8,9,11,17,18	2 ⁻
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,7,10,14,16	4,6,8,9,11	2 ⁻
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,7,10,14,17	4,6,8,9,11,15,17	2 ⁻
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,7,10,14,16,18	4,6,8,9,11,15,18	2 ⁻
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,7,10,18	4,6,8,9,11,13,18	2 ⁻
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,7,10,16,17	4,6,8,9,11,13,17	2 ⁻
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,7,10	4,6,8,9,11,13,15	2 ⁻
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,7,10,16,17,18	4,6,8,9,11,13,15,17,18	2 ⁻
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,7,10,14,17	4,6,8,9,11,13,17	2 ⁻
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,7,10,14,16,18	4,6,8,9,11,13,18	2 ⁻
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,7,10,14,17,18	4,6,8,9,11,13,15,17,18	2 ⁻
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,7,10,14,16	4,6,8,9,11,13,15	2 ⁻
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,7,10,12,17,18	4,6,8,9,11,17,18	2 ⁻
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,7,10,12,16	4,6,8,9,11	2 ⁻
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,7,10,12,17	4,6,8,9,11,15,17	2 ⁻
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,7,10,12,16,18	4,6,8,9,11,15,18	2 ⁻
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,7,10,12,14	4,6,8,9,11	2 ⁻
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,7,10,12,14,16,17,18	4,6,8,9,11,17,18	2 ⁻
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,7,10,12,14,18	4,6,8,9,11,15,18	2 ⁻
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,7,10,12,14,16,17	4,6,8,9,11,15,17	2 ⁻
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,7,10,12,17	4,6,8,9,11,13,17	2 ⁻
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,7,10,12,16,18	4,6,8,9,11,13,18	2 ⁻
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,7,10,12,17,18	4,6,8,9,11,13,15,17,18	2 ⁻
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,7,10,12,16	4,6,8,9,11,13,15	2 ⁻
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,7,10,12,14,18	4,6,8,9,11,13,18	2 ⁻
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,10,12,14,16,17	4,6,8,9,11,13,17	2 ⁻
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,7,10,12,14,16,17	4,6,8,9,11,13,17	2 ⁻
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,7,10,12,14	4,6,8,9,11,13,15	2 ⁻
$(1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,10,12,14,16,17,18	4,6,8,9,11,13,15,17,18	2 ⁻

Table 0.1537 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,17	2,17	2^{-1}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,16,18	2,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,17,18	2,15,17,18	2^{-1}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,16	2,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,14,18	2,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,14,16,17	2,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,14	2,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,14,16,17,18	2,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,17,18	2,13,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,16	2,13	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,17	2,13,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,16,18	2,13,15,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,14	2,13	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,14,16,17,18	2,13,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,14,18	2,13,15,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,14,16,17	2,13,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,12,18	2,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,12,16,17	2,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,12	2,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,12,16,17,18	2,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,12,14,17	2,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,12,14,16,18	2,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,12,14,17,18	2,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,12,14,16	2,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,12	2,13	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,12,16,17,18	2,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,12,18	2,13,15,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,12,16,17	2,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,12,14,17,18	2,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,12,14,16	2,13	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,12,14,17	2,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,12,14,16,18	2,13,15,18	2^{-23}

Table 0.1538 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,17,18	2,11,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,16	2,11	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,17	2,11,15,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,16,18	2,11,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,14	2,11	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,14,16,17,18	2,11,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,14,18	2,11,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,14,16,17	2,11,15,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,17	2,11,13,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,16,18	2,11,13,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,17,18	2,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,16	2,11,13,15	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,14,18	2,11,13,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,14,16,17	2,11,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,14	2,11,13,15	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,14,16,17,18	2,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,12	2,11	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,12,16,17,18	2,11,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,12,18	2,11,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,12,16,17	2,11,15,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,12,14,17,18	2,11,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,12,14,16	2,11	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,12,14,17	2,11,15,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,12,14,16,18	2,11,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,12,18	2,11,13,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,12,16,17	2,11,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,12	2,11,13,15	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,12,16,17,18	2,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,12,14,17	2,11,13,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,12,14,16,18	2,11,13,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,12,14,17,18	2,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,12,14,16	2,11,13,15	2^{-12}

Table 0.1539 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,10,18	2,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,10,16,17	2,17	2^{-34}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,10	2,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,10,16,17,18	2,15,17,18	2^{-34}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,10,14,17	2,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,10,14,16,18	2,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,10,14,17,18	2,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,10,14,16	2,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,10	2,13	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,10,16,17,18	2,13,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,10,18	2,13,15,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,10,16,17	2,13,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,10,14,17,18	2,13,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,10,14,16	2,13	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,10,14,17	2,13,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,10,14,16,18	2,13,15,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,10,12,17	2,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,10,12,16,18	2,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,10,12,17,18	2,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,10,12,16	2,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,10,12,14,18	2,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,10,12,14,16,17	2,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,10,12,14	2,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,10,12,14,16,17,18	2,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,10,12,17,18	2,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,10,12,16	2,13	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,10,12,17	2,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,10,12,16,18	2,13,15,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,10,12,14	2,13	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,10,12,14,16,17,18	2,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,10,12,14,18	2,13,15,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,10,12,14,16,17	2,13,15,17	$2^{-17.5}$

Table 0.1540 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,10	2,11	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,10,16,17,18	2,11,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,10,18	2,11,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,10,16,17	2,11,15,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,10,14,17,18	2,11,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,10,14,16	2,11	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,10,14,17	2,11,15,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,10,14,16,18	2,11,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,10,18	2,11,13,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,10,16,17	2,11,13,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,10	2,11,13,15	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,10,16,17,18	2,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,10,14,17	2,11,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,10,14,16,18	2,11,13,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,10,14,17,18	2,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,10,14,16	2,11,13,15	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,10,12,17,18	2,11,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,10,12,16	2,11	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,10,12,17	2,11,15,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,10,12,16,18	2,11,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,10,12,14	2,11	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,10,12,14,16,17,18	2,11,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,10,12,14,18	2,11,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,10,12,14,16,17	2,11,15,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,10,12,17	2,11,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,10,12,16,18	2,11,13,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,10,12,17,18	2,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,10,12,16	2,11,13,15	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,10,12,14,18	2,11,13,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,10,12,14,16,17	2,11,13,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,10,12,14	2,11,13,15	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,10,12,14,16,17,18	2,11,13,15,17,18	$2^{-28.5}$

Table 0.1541 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,17,18	2,9,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,16	2,9	2^{-34}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,17	2,9,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,16,18	2,9,15,18	2^{-34}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,14	2,9	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,14,16,17,18	2,9,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,14,18	2,9,15,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,14,16,17	2,9,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,17	2,9,13,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,16,18	2,9,13,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,17,18	2,9,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,16	2,9,13,15	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,14,18	2,9,13,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,14,16,17	2,9,13,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,14	2,9,13,15	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,14,16,17,18	2,9,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,12	2,9	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,12,16,17,18	2,9,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,12,18	2,9,15,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,12,16,17	2,9,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,12,14,17,18	2,9,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,12,14,16	2,9	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,12,14,17	2,9,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,12,14,16,18	2,9,15,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,12,18	2,9,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,12,16,17	2,9,13,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,12	2,9,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,12,16,17,18	2,9,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,12,14,17	2,9,13,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,12,14,16,18	2,9,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,12,14,17,18	2,9,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,12,14,16	2,9,13,15	$2^{-17.5}$

Table 0.1542 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,17	2,9,11,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,16,18	2,9,11,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,17,18	2,9,11,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,16	2,9,11,15	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,14,18	2,9,11,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,14,16,17	2,9,11,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,14	2,9,11,15	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,14,16,17,18	2,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,17,18	2,9,11,13,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,16	2,9,11,13	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,17	2,9,11,13,15,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,16,18	2,9,11,13,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,14	2,9,11,13	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,14,16,17,18	2,9,11,13,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,14,18	2,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,14,16,17	2,9,11,13,15,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,12,18	2,9,11,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,12,16,17	2,9,11,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,12	2,9,11,15	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,12,16,17,18	2,9,11,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,12,14,17	2,9,11,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,12,14,16,18	2,9,11,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,12,14,17,18	2,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,12,14,16	2,9,11,15	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,12	2,9,11,13	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,12,16,17,18	2,9,11,13,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,12,18	2,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,12,16,17	2,9,11,13,15,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,12,14,17,18	2,9,11,13,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,12,14,16	2,9,11,13	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,12,14,17	2,9,11,13,15,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,12,14,16,18	2,9,11,13,15,18	$2^{-28.5}$

Table 0.1543 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,10	2,9	2^{-1}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,10,16,17,18	2,9,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,10,18	2,9,15,18	2^{-1}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,10,16,17	2,9,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,10,14,17,18	2,9,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,10,14,16	2,9	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,10,14,17	2,9,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,10,14,16,18	2,9,15,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,10,18	2,9,13,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,10,16,17	2,9,13,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,10	2,9,13,15	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,10,16,17,18	2,9,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,10,14,17	2,9,13,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,10,14,16,18	2,9,13,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,10,14,17,18	2,9,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,10,14,16	2,9,13,15	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,10,12,17,18	2,9,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,10,12,16	2,9	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,10,12,17	2,9,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,10,12,16,18	2,9,15,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,10,12,14	2,9	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,10,12,14,16,17,18	2,9,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,10,12,14,18	2,9,15,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,10,12,14,16,17	2,9,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,10,12,17	2,9,13,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,10,12,16,18	2,9,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,10,12,17,18	2,9,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,10,12,16	2,9,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,10,12,14,18	2,9,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,10,12,14,16,17	2,9,13,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,10,12,14	2,9,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,10,12,14,16,17,18	2,9,13,15,17,18	2^{-23}

Table 0.1544 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,10,18	2,9,11,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,10,16,17	2,9,11,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,10	2,9,11,15	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,10,16,17,18	2,9,11,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,10,14,17	2,9,11,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,10,14,16,18	2,9,11,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,10,14,17,18	2,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,10,14,16	2,9,11,15	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,10	2,9,11,13	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,10,16,17,18	2,9,11,13,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,10,18	2,9,11,13,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,10,16,17	2,9,11,13,15,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,10,14,17,18	2,9,11,13,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,10,14,16	2,9,11,13	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,10,14,17	2,9,11,13,15,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,10,14,16,18	2,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,10,12,17	2,9,11,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,10,12,16,18	2,9,11,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,10,12,17,18	2,9,11,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,10,12,16	2,9,11,15	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,10,12,14,18	2,9,11,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,10,12,14,16,17	2,9,11,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,10,12,14	2,9,11,15	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,10,12,14,16,17,18	2,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,10,12,17,18	2,9,11,13,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,10,12,16	2,9,11,13	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,10,12,17	2,9,11,13,15,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,10,12,16,18	2,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,10,12,14	2,9,11,13	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,10,12,14,16,17,18	2,9,11,13,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,10,12,14,18	2,9,11,13,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,10,12,14,16,17	2,9,11,13,15,17	2^{-12}

Table 0.1545 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,18	2,8,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,16,17	2,8,17	2^{-1}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1	2,8,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,16,17,18	2,8,15,17,18	2^{-1}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,14,17	2,8,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,14,16,18	2,8,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,14,17,18	2,8,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,14,16	2,8,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1	2,8,13	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,16,17,18	2,8,13,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,18	2,8,13,15,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,16,17	2,8,13,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,14,17,18	2,8,13,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,14,16	2,8,13	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,14,17	2,8,13,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,14,16,18	2,8,13,15,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,12,17	2,8,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,12,16,18	2,8,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,12,17,18	2,8,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,12,16	2,8,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,12,14,18	2,8,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,12,14,16,17	2,8,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,12,14	2,8,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,12,14,16,17,18	2,8,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,12,17,18	2,8,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,12,16	2,8,13	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,12,17	2,8,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,12,16,18	2,8,13,15,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,12,14	2,8,13	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,12,14,16,17,18	2,8,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,12,14,18	2,8,13,15,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,12,14,16,17	2,8,13,15,17	$2^{-17.5}$

Table 0.1546 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1	2,8,11	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,16,17,18	2,8,11,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,18	2,8,11,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,16,17	2,8,11,15,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,14,17,18	2,8,11,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,14,16	2,8,11	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,14,17	2,8,11,15,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,14,16,18	2,8,11,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,18	2,8,11,13,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,16,17	2,8,11,13,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1	2,8,11,13,15	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,16,17,18	2,8,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,14,17	2,8,11,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,14,16,18	2,8,11,13,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,14,17,18	2,8,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,14,16	2,8,11,13,15	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,12,17,18	2,8,11,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,12,16	2,8,11	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,12,17	2,8,11,15,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,12,16,18	2,8,11,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,12,14	2,8,11	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,12,14,16,17,18	2,8,11,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,12,14,18	2,8,11,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,12,14,16,17	2,8,11,15,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,12,17	2,8,11,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,12,16,18	2,8,11,13,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,12,17,18	2,8,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,12,16	2,8,11,13,15	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,12,14,18	2,8,11,13,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,12,14,16,17	2,8,11,13,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,12,14	2,8,11,13,15	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,12,14,16,17,18	2,8,11,13,15,17,18	$2^{-6.5}$

Table 0.1547 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(2)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,10,17	2,8,17	2^{-34}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,10,16,18	2,8,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,10,17,18	2,8,15,17,18	2^{-34}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,10,16	2,8,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,10,14,18	2,8,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,10,14,16,17	2,8,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,10,14	2,8,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,10,14,16,17,18	2,8,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,10,17,18	2,8,13,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,10,16	2,8,13	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,10,17	2,8,13,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1)$	1,10,16,18	2,8,13,15,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,10,14	2,8,13	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,10,14,16,17,18	2,8,13,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,10,14,18	2,8,13,15,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,10,14,16,17	2,8,13,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,10,12,18	2,8,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,10,12,16,17	2,8,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,10,12	2,8,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,10,12,16,17,18	2,8,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,10,12,14,17	2,8,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,10,12,14,16,18	2,8,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,10,12,14,17,18	2,8,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,10,12,14,16	2,8,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,10,12	2,8,13	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,10,12,16,17,18	2,8,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,10,12,18	2,8,13,15,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,10,12,16,17	2,8,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,10,12,14,17,18	2,8,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,10,12,14,16	2,8,13	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,10,12,14,17	2,8,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,10,12,14,16,18	2,8,13,15,18	2^{-12}

Table 0.1548 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,10,17,18	2,8,11,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,10,16	2,8,11	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,10,17	2,8,11,15,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,10,16,18	2,8,11,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,10,14	2,8,11	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,10,14,16,17,18	2,8,11,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,10,14,18	2,8,11,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,10,14,16,17	2,8,11,15,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,10,17	2,8,11,13,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,10,16,18	2,8,11,13,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,10,17,18	2,8,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,10,16	2,8,11,13,15	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,10,14,18	2,8,11,13,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,10,14,16,17	2,8,11,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,10,14	2,8,11,13,15	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,10,14,16,17,18	2,8,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,10,12	2,8,11	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,10,12,16,17,18	2,8,11,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,10,12,18	2,8,11,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,10,12,16,17	2,8,11,15,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,10,12,14,17,18	2,8,11,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,10,12,14,16	2,8,11	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,10,12,14,17	2,8,11,15,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,10,12,14,16,18	2,8,11,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,10,12,18	2,8,11,13,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,10,12,16,17	2,8,11,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,10,12	2,8,11,13,15	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,10,12,16,17,18	2,8,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,10,12,14,17	2,8,11,13,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,10,12,14,16,18	2,8,11,13,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,10,12,14,17,18	2,8,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,10,12,14,16	2,8,11,13,15	2^{-23}

Table 0.1549 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1	2,8,9	2^{-34}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,16,17,18	2,8,9,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,18	2,8,9,15,18	2^{-34}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,16,17	2,8,9,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,14,17,18	2,8,9,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,14,16	2,8,9	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,14,17	2,8,9,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,14,16,18	2,8,9,15,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,18	2,8,9,13,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,16,17	2,8,9,13,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1	2,8,9,13,15	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,16,17,18	2,8,9,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,14,17	2,8,9,13,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,14,16,18	2,8,9,13,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,14,17,18	2,8,9,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,14,16	2,8,9,13,15	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,12,17,18	2,8,9,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,12,16	2,8,9	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,12,17	2,8,9,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,12,16,18	2,8,9,15,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,12,14	2,8,9	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,12,14,16,17,18	2,8,9,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,12,14,18	2,8,9,15,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,12,14,16,17	2,8,9,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,12,17	2,8,9,13,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,12,16,18	2,8,9,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,12,17,18	2,8,9,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,12,16	2,8,9,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,12,14,18	2,8,9,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,12,14,16,17	2,8,9,13,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,12,14	2,8,9,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,12,14,16,17,18	2,8,9,13,15,17,18	2^{-12}

Table 0.1550 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,18	2,8,9,11,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,16,17	2,8,9,11,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1	2,8,9,11,15	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,16,17,18	2,8,9,11,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,14,17	2,8,9,11,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,14,16,18	2,8,9,11,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,14,17,18	2,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,14,16	2,8,9,11,15	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1	2,8,9,11,13	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,16,17,18	2,8,9,11,13,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,18	2,8,9,11,13,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,16,17	2,8,9,11,13,15,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,14,17,18	2,8,9,11,13,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,14,16	2,8,9,11,13	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,14,17	2,8,9,11,13,15,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,14,16,18	2,8,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,12,17	2,8,9,11,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,12,16,18	2,8,9,11,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,12,17,18	2,8,9,11,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,12,16	2,8,9,11,15	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,12,14,18	2,8,9,11,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,12,14,16,17	2,8,9,11,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,12,14	2,8,9,11,15	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,12,14,16,17,18	2,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,12,17,18	2,8,9,11,13,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,12,16	2,8,9,11,13	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,12,17	2,8,9,11,13,15,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,12,16,18	2,8,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,12,14	2,8,9,11,13	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,12,14,16,17,18	2,8,9,11,13,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,12,14,18	2,8,9,11,13,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,12,14,16,17	2,8,9,11,13,15,17	2^{-23}

Table 0.1551 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,10,17,18	2,8,9,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,10,16	2,8,9	2^{-1}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,10,17	2,8,9,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,10,16,18	2,8,9,15,18	2^{-1}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,10,14	2,8,9	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,10,14,16,17,18	2,8,9,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,10,14,18	2,8,9,15,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,10,14,16,17	2,8,9,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,10,17	2,8,9,13,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,10,16,18	2,8,9,13,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,10,17,18	2,8,9,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,10,16	2,8,9,13,15	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,10,14,18	2,8,9,13,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,10,14,16,17	2,8,9,13,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,10,14	2,8,9,13,15	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,10,14,16,17,18	2,8,9,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,10,12	2,8,9	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,10,12,16,17,18	2,8,9,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,10,12,18	2,8,9,15,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,10,12,16,17	2,8,9,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,10,12,14,17,18	2,8,9,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,10,12,14,16	2,8,9	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,10,12,14,17	2,8,9,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,10,12,14,16,18	2,8,9,15,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,10,12,18	2,8,9,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,10,12,16,17	2,8,9,13,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,10,12	2,8,9,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,10,12,16,17,18	2,8,9,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,10,12,14,17	2,8,9,13,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,10,12,14,16,18	2,8,9,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,10,12,14,17,18	2,8,9,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,10,12,14,16	2,8,9,13,15	$2^{-17.5}$

Table 0.1552 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,10,17	2,8,9,11,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,10,16,18	2,8,9,11,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,10,17,18	2,8,9,11,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,10,16	2,8,9,11,15	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,10,14,18	2,8,9,11,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,10,14,16,17	2,8,9,11,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,10,14	2,8,9,11,15	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,10,14,16,17,18	2,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,10,17,18	2,8,9,11,13,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,10,16	2,8,9,11,13	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,10,17	2,8,9,11,13,15,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,10,16,18	2,8,9,11,13,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,10,14	2,8,9,11,13	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,10,14,16,17,18	2,8,9,11,13,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,10,14,18	2,8,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,10,14,16,17	2,8,9,11,13,15,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,10,12,18	2,8,9,11,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,10,12,16,17	2,8,9,11,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,10,12	2,8,9,11,15	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,10,12,16,17,18	2,8,9,11,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,10,12,14,17	2,8,9,11,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,10,12,14,16,18	2,8,9,11,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,10,12,14,17,18	2,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,10,12,14,16	2,8,9,11,15	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,10,12	2,8,9,11,13	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,10,12,16,17,18	2,8,9,11,13,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,10,12,18	2,8,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,10,12,16,17	2,8,9,11,13,15,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,10,12,14,17,18	2,8,9,11,13,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,10,12,14,16	2,8,9,11,13	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,10,12,14,17	2,8,9,11,13,15,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,10,12,14,16,18	2,8,9,11,13,15,18	$2^{-6.5}$

Table 0.1553 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,7,17,18	2,17,18	2^{-1}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,7,16	2	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,7,17	2,15,17	2^{-1}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,7,16,18	2,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,7,14	2	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,7,14,16,17,18	2,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0)$	1,7,14,18	2,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,7,14,16,17	2,15,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,7,17	2,13,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,7,16,18	2,13,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,7,17,18	2,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,7,16	2,13,15	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,7,14,18	2,13,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,7,14,16,17	2,13,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,7,14	2,13,15	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,7,14,16,17,18	2,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,7,12	2	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,7,12,16,17,18	2,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,7,12,18	2,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,7,12,16,17	2,15,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,7,12,14,17,18	2,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,7,12,14,16	2	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,7,12,14,17	2,15,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,7,12,14,16,18	2,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,7,12,18	2,13,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,7,12,16,17	2,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,7,12	2,13,15	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,7,12,16,17,18	2,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,7,12,14,17	2,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,7,12,14,16,18	2,13,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,7,12,14,17,18	2,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,7,12,14,16	2,13,15	2^{-23}

Table 0.1554 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,7,17	2,11,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,7,16,18	2,11,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,7,17,18	2,11,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,7,16	2,11,15	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,7,14,18	2,11,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,7,14,16,17	2,11,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,7,14	2,11,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,7,14,16,17,18	2,11,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,7,17,18	2,11,13,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,7,16	2,11,13	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,7,17	2,11,13,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,7,16,18	2,11,13,15,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,7,14	2,11,13	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,7,14,16,17,18	2,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,7,14,18	2,11,13,15,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,7,14,16,17	2,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,7,12,18	2,11,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,7,12,16,17	2,11,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,7,12	2,11,15	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,7,12,16,17,18	2,11,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,7,12,14,17	2,11,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,7,12,14,16,18	2,11,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,7,12,14,17,18	2,11,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,7,12,14,16	2,11,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,7,12	2,11,13	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,7,12,16,17,18	2,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,7,12,18	2,11,13,15,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,7,12,16,17	2,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,7,12,14,17,18	2,11,13,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,7,12,14,16	2,11,13	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,7,12,14,17	2,11,13,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,7,12,14,16,18	2,11,13,15,18	2^{-12}

Table 0.1555 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,7,10	2	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,7,10,16,17,18	2,17,18	2^{-34}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,7,10,18	2,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,7,10,16,17	2,15,17	2^{-34}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,7,10,14,17,18	2,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,7,10,14,16	2	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,7,10,14,17	2,15,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,7,10,14,16,18	2,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,7,10,18	2,13,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,7,10,16,17	2,13,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,7,10	2,13,15	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,7,10,16,17,18	2,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,7,10,14,17	2,13,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,7,10,14,16,18	2,13,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,7,10,14,17,18	2,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,7,10,14,16	2,13,15	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,7,10,12,17,18	2,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,7,10,12,16	2	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,7,10,12,17	2,15,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,7,10,12,16,18	2,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,7,10,12,14	2	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,7,10,12,14,16,17,18	2,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,7,10,12,14,18	2,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,7,10,12,14,16,17	2,15,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,7,10,12,17	2,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,7,10,12,16,18	2,13,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,7,10,12,17,18	2,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,7,10,12,16	2,13,15	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,7,10,12,14,18	2,13,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,7,10,12,14,16,17	2,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,7,10,12,14	2,13,15	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,7,10,12,14,16,17,18	2,13,15,17,18	$2^{-17.5}$

Table 0.1556 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,7,10,18	2,11,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,7,10,16,17	2,11,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,7,10	2,11,15	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,7,10,16,17,18	2,11,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,7,10,14,17	2,11,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,7,10,14,16,18	2,11,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,7,10,14,17,18	2,11,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,7,10,14,16	2,11,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,7,10	2,11,13	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,7,10,16,17,18	2,11,13,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,7,10,18	2,11,13,15,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,7,10,16,17	2,11,13,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,7,10,14,17,18	2,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,7,10,14,16	2,11,13	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,7,10,14,17	2,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,7,10,14,16,18	2,11,13,15,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,7,10,12,17	2,11,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,7,10,12,16,18	2,11,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,7,10,12,17,18	2,11,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,7,10,12,16	2,11,15	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,7,10,12,14,18	2,11,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,7,10,12,14,16,17	2,11,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,7,10,12,14	2,11,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,7,10,12,14,16,17,18	2,11,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,7,10,12,17,18	2,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,7,10,12,16	2,11,13	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,7,10,12,17	2,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,7,10,12,16,18	2,11,13,15,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,7,10,12,14	2,11,13	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,7,10,12,14,16,17,18	2,11,13,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,7,10,12,14,18	2,11,13,15,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,7,10,12,14,16,17	2,11,13,15,17	$2^{-28.5}$

Table 0.1557 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,7,17	2,9,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,7,16,18	2,9,18	2^{-34}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,7,17,18	2,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,7,16	2,9,15	2^{-34}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,7,14,18	2,9,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,7,14,16,17	2,9,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0)$	1,7,14	2,9,15	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,7,14,16,17,18	2,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,7,17,18	2,9,13,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,7,16	2,9,13	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,7,17	2,9,13,15,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,7,16,18	2,9,13,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,7,14	2,9,13	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,7,14,16,17,18	2,9,13,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,7,14,18	2,9,13,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,7,14,16,17	2,9,13,15,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,7,12,18	2,9,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,7,12,16,17	2,9,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,7,12	2,9,15	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,7,12,16,17,18	2,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,7,12,14,17	2,9,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,7,12,14,16,18	2,9,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,7,12,14,17,18	2,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,7,12,14,16	2,9,15	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,7,12	2,9,13	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,7,12,16,17,18	2,9,13,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,7,12,18	2,9,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,7,12,16,17	2,9,13,15,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,7,12,14,17,18	2,9,13,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,7,12,14,16	2,9,13	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,7,12,14,17	2,9,13,15,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,7,12,14,16,18	2,9,13,15,18	$2^{-17.5}$

Table 0.1558 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,7,17,18	2,9,11,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,7,16	2,9,11	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,7,17	2,9,11,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,7,16,18	2,9,11,15,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,7,14	2,9,11	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,7,14,16,17,18	2,9,11,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,7,14,18	2,9,11,15,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,7,14,16,17	2,9,11,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,7,17	2,9,11,13,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,7,16,18	2,9,11,13,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,7,17,18	2,9,11,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,7,16	2,9,11,13,15	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,7,14,18	2,9,11,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,7,14,16,17	2,9,11,13,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,7,14	2,9,11,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,7,14,16,17,18	2,9,11,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,7,12	2,9,11	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,7,12,16,17,18	2,9,11,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,7,12,18	2,9,11,15,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,7,12,16,17	2,9,11,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,7,12,14,17,18	2,9,11,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,7,12,14,16	2,9,11	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,7,12,14,17	2,9,11,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,7,12,14,16,18	2,9,11,15,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,7,12,18	2,9,11,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,7,12,16,17	2,9,11,13,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,7,12	2,9,11,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,7,12,16,17,18	2,9,11,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,7,12,14,17	2,9,11,13,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,7,12,14,16,18	2,9,11,13,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,7,12,14,17,18	2,9,11,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,7,12,14,16	2,9,11,13,15	$2^{-28.5}$

Table 0.1559 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,7,10,18	2,9,18	2^{-1}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,7,10,16,17	2,9,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,7,10	2,9,15	2^{-1}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,7,10,16,17,18	2,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,7,10,14,17	2,9,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,7,10,14,16,18	2,9,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,7,10,14,17,18	2,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,7,10,14,16	2,9,15	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,7,10	2,9,13	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,7,10,16,17,18	2,9,13,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,7,10,18	2,9,13,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,7,10,16,17	2,9,13,15,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,7,10,14,17,18	2,9,13,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,7,10,14,16	2,9,13	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,7,10,14,17	2,9,13,15,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,7,10,14,16,18	2,9,13,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,7,10,12,17	2,9,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,7,10,12,16,18	2,9,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,7,10,12,17,18	2,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,7,10,12,16	2,9,15	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,7,10,12,14,18	2,9,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,7,10,12,14,16,17	2,9,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,7,10,12,14	2,9,15	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,7,10,12,14,16,17,18	2,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,7,10,12,17,18	2,9,13,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,7,10,12,16	2,9,13	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,7,10,12,17	2,9,13,15,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,7,10,12,16,18	2,9,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,7,10,12,14	2,9,13	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,7,10,12,14,16,17,18	2,9,13,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,7,10,12,14,18	2,9,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,7,10,12,14,16,17	2,9,13,15,17	2^{-23}

Table 0.1560 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,7,10	2,9,11	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,7,10,16,17,18	2,9,11,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,7,10,18	2,9,11,15,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,7,10,16,17	2,9,11,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,7,10,14,17,18	2,9,11,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,7,10,14,16	2,9,11	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,7,10,14,17	2,9,11,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,7,10,14,16,18	2,9,11,15,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,7,10,18	2,9,11,13,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,7,10,16,17	2,9,11,13,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,7,10	2,9,11,13,15	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,7,10,16,17,18	2,9,11,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,7,10,14,17	2,9,11,13,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,7,10,14,16,18	2,9,11,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,7,10,14,17,18	2,9,11,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,7,10,14,16	2,9,11,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,7,10,12,17,18	2,9,11,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,7,10,12,16	2,9,11	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,7,10,12,17	2,9,11,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,7,10,12,16,18	2,9,11,15,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,7,10,12,14	2,9,11	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,7,10,12,14,16,17,18	2,9,11,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,7,10,12,14,18	2,9,11,15,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,7,10,12,14,16,17	2,9,11,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,7,10,12,17	2,9,11,13,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,7,10,12,16,18	2,9,11,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,7,10,12,17,18	2,9,11,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,7,10,12,16	2,9,11,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,7,10,12,14,18	2,9,11,13,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,7,10,12,14,16,17	2,9,11,13,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,7,10,12,14	2,9,11,13,15	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,7,10,12,14,16,17,18	2,9,11,13,15,17,18	2^{-12}

Table 0.1561 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,7	2,8	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,7,16,17,18	2,8,17,18	2^{-1}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,7,18	2,8,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,7,16,17	2,8,15,17	2^{-1}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,7,14,17,18	2,8,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,7,14,16	2,8	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,7,14,17	2,8,15,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,7,14,16,18	2,8,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,7,18	2,8,13,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,7,16,17	2,8,13,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,7	2,8,13,15	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,7,16,17,18	2,8,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,7,14,17	2,8,13,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,7,14,16,18	2,8,13,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,7,14,17,18	2,8,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,7,14,16	2,8,13,15	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,7,12,17,18	2,8,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,7,12,16	2,8	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,7,12,17	2,8,15,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,7,12,16,18	2,8,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,7,12,14	2,8	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,7,12,14,16,17,18	2,8,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,7,12,14,18	2,8,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,7,12,14,16,17	2,8,15,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,7,12,17	2,8,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1)$	1,7,12,16,18	2,8,13,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,7,12,17,18	2,8,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,7,12,16	2,8,13,15	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,7,12,14,18	2,8,13,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,7,12,14,16,17	2,8,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,7,12,14	2,8,13,15	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,7,12,14,16,17,18	2,8,13,15,17,18	$2^{-17.5}$

Table 0.1562 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,7,18	2,8,11,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,7,16,17	2,8,11,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,7	2,8,11,15	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,7,16,17,18	2,8,11,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,7,14,17	2,8,11,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,7,14,16,18	2,8,11,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,7,14,17,18	2,8,11,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,7,14,16	2,8,11,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,7	2,8,11,13	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,7,16,17,18	2,8,11,13,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,7,18	2,8,11,13,15,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,7,16,17	2,8,11,13,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,7,14,17,18	2,8,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,7,14,16	2,8,11,13	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,7,14,17	2,8,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,7,14,16,18	2,8,11,13,15,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,7,12,17	2,8,11,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,7,12,16,18	2,8,11,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,7,12,17,18	2,8,11,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,7,12,16	2,8,11,15	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,7,12,14,18	2,8,11,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,7,12,14,16,17	2,8,11,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,7,12,14	2,8,11,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,7,12,14,16,17,18	2,8,11,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,7,12,17,18	2,8,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,7,12,16	2,8,11,13	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,7,12,17	2,8,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,7,12,16,18	2,8,11,13,15,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,7,12,14	2,8,11,13	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,7,12,14,16,17,18	2,8,11,13,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,7,12,14,18	2,8,11,13,15,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,7,12,14,16,17	2,8,11,13,15,17	$2^{-6.5}$

Table 0.1563 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,7,10,17,18	2,8,17,18	2^{-34}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,7,10,16	2,8	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,7,10,17	2,8,15,17	2^{-34}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,7,10,16,18	2,8,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,7,10,14	2,8	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,7,10,14,16,17,18	2,8,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,7,10,14,18	2,8,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,7,10,14,16,17	2,8,15,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,7,10,17	2,8,13,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,7,10,16,18	2,8,13,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,7,10,17,18	2,8,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,7,10,16	2,8,13,15	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,7,10,14,18	2,8,13,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,7,10,14,16,17	2,8,13,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,7,10,14	2,8,13,15	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,7,10,14,16,17,18	2,8,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,7,10,12	2,8	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,7,10,12,16,17,18	2,8,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,7,10,12,18	2,8,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,7,10,12,16,17	2,8,15,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,7,10,12,14,17,18	2,8,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0)$	1,7,10,12,14,16	2,8	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,7,10,12,14,17	2,8,15,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,7,10,12,14,16,18	2,8,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,7,10,12,18	2,8,13,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,7,10,12,16,17	2,8,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,7,10,12	2,8,13,15	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,7,10,12,16,17,18	2,8,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,7,10,12,14,17	2,8,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,7,10,12,14,16,18	2,8,13,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,7,10,12,14,17,18	2,8,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,7,10,12,14,16	2,8,13,15	2^{-12}

Table 0.1564 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,7,10,17	2,8,11,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,7,10,16,18	2,8,11,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,7,10,17,18	2,8,11,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,7,10,16	2,8,11,15	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,7,10,14,18	2,8,11,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,7,10,14,16,17	2,8,11,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,7,10,14	2,8,11,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,7,10,14,16,17,18	2,8,11,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,7,10,17,18	2,8,11,13,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,7,10,16	2,8,11,13	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,7,10,17	2,8,11,13,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,7,10,16,18	2,8,11,13,15,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,7,10,14	2,8,11,13	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,7,10,14,16,17,18	2,8,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,7,10,14,18	2,8,11,13,15,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,7,10,14,16,17	2,8,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,7,10,12,18	2,8,11,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,7,10,12,16,17	2,8,11,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,7,10,12	2,8,11,15	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,7,10,12,16,17,18	2,8,11,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,7,10,12,14,17	2,8,11,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,7,10,12,14,16,18	2,8,11,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,7,10,12,14,17,18	2,8,11,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,7,10,12,14,16	2,8,11,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,7,10,12	2,8,11,13	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,7,10,12,16,17,18	2,8,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,7,10,12,18	2,8,11,13,15,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,7,10,12,16,17	2,8,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,7,10,12,14,17,18	2,8,11,13,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,7,10,12,14,16	2,8,11,13	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,7,10,12,14,17	2,8,11,13,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,7,10,12,14,16,18	2,8,11,13,15,18	2^{-23}

Table 0.1565 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,7,18	2,8,9,18	2^{-34}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,7,16,17	2,8,9,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,7	2,8,9,15	2^{-34}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,7,16,17,18	2,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,7,14,17	2,8,9,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,7,14,16,18	2,8,9,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,7,14,17,18	2,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,7,14,16	2,8,9,15	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,7	2,8,9,13	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,7,16,17,18	2,8,9,13,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,7,18	2,8,9,13,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,7,16,17	2,8,9,13,15,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,7,14,17,18	2,8,9,13,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,7,14,16	2,8,9,13	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,7,14,17	2,8,9,13,15,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,7,14,16,18	2,8,9,13,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,7,12,17	2,8,9,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,7,12,16,18	2,8,9,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,7,12,17,18	2,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,7,12,16	2,8,9,15	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,7,12,14,18	2,8,9,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,7,12,14,16,17	2,8,9,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,7,12,14	2,8,9,15	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,7,12,14,16,17,18	2,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,7,12,17,18	2,8,9,13,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,7,12,16	2,8,9,13	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,7,12,17	2,8,9,13,15,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,7,12,16,18	2,8,9,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,7,12,14	2,8,9,13	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,7,12,14,16,17,18	2,8,9,13,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,7,12,14,18	2,8,9,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,7,12,14,16,17	2,8,9,13,15,17	2^{-12}

Table 0.1566 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,7	2,8,9,11	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,7,16,17,18	2,8,9,11,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,7,18	2,8,9,11,15,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,7,16,17	2,8,9,11,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,7,14,17,18	2,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,7,14,16	2,8,9,11	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,7,14,17	2,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,7,14,16,18	2,8,9,11,15,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,7,18	2,8,9,11,13,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,7,16,17	2,8,9,11,13,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,7	2,8,9,11,13,15	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,7,16,17,18	2,8,9,11,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,7,14,17	2,8,9,11,13,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,7,14,16,18	2,8,9,11,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,7,14,17,18	2,8,9,11,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,7,14,16	2,8,9,11,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,7,12,17,18	2,8,9,11,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,7,12,16	2,8,9,11	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,7,12,17	2,8,9,11,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,7,12,16,18	2,8,9,11,15,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,7,12,14	2,8,9,11	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,7,12,14,16,17,18	2,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,7,12,14,18	2,8,9,11,15,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,7,12,14,16,17	2,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,7,12,17	2,8,9,11,13,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,7,12,16,18	2,8,9,11,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,7,12,17,18	2,8,9,11,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,7,12,16	2,8,9,11,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,7,12,14,18	2,8,9,11,13,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,7,12,14,16,17	2,8,9,11,13,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,7,12,14	2,8,9,11,13,15	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,7,12,14,16,17,18	2,8,9,11,13,15,17,18	2^{-23}

Table 0.1567 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,7,10,17	2,8,9,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,7,10,16,18	2,8,9,18	2^{-1}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,7,10,17,18	2,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,7,10,16	2,8,9,15	2^{-1}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,7,10,14,18	2,8,9,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,7,10,14,16,17	2,8,9,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,7,10,14	2,8,9,15	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,7,10,14,16,17,18	2,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,7,10,17,18	2,8,9,13,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,7,10,16	2,8,9,13	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,7,10,17	2,8,9,13,15,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,7,10,16,18	2,8,9,13,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,7,10,14	2,8,9,13	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,7,10,14,16,17,18	2,8,9,13,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,7,10,14,18	2,8,9,13,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,7,10,14,16,17	2,8,9,13,15,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,7,10,12,18	2,8,9,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,7,10,12,16,17	2,8,9,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,7,10,12	2,8,9,15	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,7,10,12,16,17,18	2,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,7,10,12,14,17	2,8,9,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,7,10,12,14,16,18	2,8,9,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,7,10,12,14,17,18	2,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,7,10,12,14,16	2,8,9,15	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,7,10,12	2,8,9,13	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,7,10,12,16,17,18	2,8,9,13,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,7,10,12,18	2,8,9,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,7,10,12,16,17	2,8,9,13,15,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,7,10,12,14,17,18	2,8,9,13,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,7,10,12,14,16	2,8,9,13	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,7,10,12,14,17	2,8,9,13,15,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,7,10,12,14,16,18	2,8,9,13,15,18	$2^{-17.5}$

Table 0.1568 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,7,10,17,18	2,8,9,11,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,7,10,16	2,8,9,11	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,7,10,17	2,8,9,11,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,7,10,16,18	2,8,9,11,15,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,7,10,14	2,8,9,11	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,7,10,14,16,17,18	2,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,7,10,14,18	2,8,9,11,15,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,7,10,14,16,17	2,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,7,10,17	2,8,9,11,13,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,7,10,16,18	2,8,9,11,13,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,7,10,17,18	2,8,9,11,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,7,10,16	2,8,9,11,13,15	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,7,10,14,18	2,8,9,11,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,7,10,14,16,17	2,8,9,11,13,17	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,7,10,14	2,8,9,11,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,7,10,14,16,17,18	2,8,9,11,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,7,10,12	2,8,9,11	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,7,10,12,16,17,18	2,8,9,11,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,7,10,12,18	2,8,9,11,15,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,7,10,12,16,17	2,8,9,11,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,7,10,12,14,17,18	2,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,7,10,12,14,16	2,8,9,11	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,7,10,12,14,17	2,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,7,10,12,14,16,18	2,8,9,11,15,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,7,10,12,18	2,8,9,11,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,7,10,12,16,17	2,8,9,11,13,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,7,10,12	2,8,9,11,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,7,10,12,16,17,18	2,8,9,11,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,7,10,12,14,17	2,8,9,11,13,17	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,7,10,12,14,16,18	2,8,9,11,13,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,7,10,12,14,17,18	2,8,9,11,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,7,10,12,14,16	2,8,9,11,13,15	$2^{-6.5}$

Table 0.1569 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,18	2,6,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,16,17	2,6,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1	2,6,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,16,17,18	2,6,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,14,17	2,6,17	2^{-1}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,14,16,18	2,6,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,14,17,18	2,6,15,17,18	2^{-1}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,14,16	2,6,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1	2,6,13	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,16,17,18	2,6,13,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,18	2,6,13,15,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,16,17	2,6,13,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,14,17,18	2,6,13,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,14,16	2,6,13	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,14,17	2,6,13,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,14,16,18	2,6,13,15,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,12,17	2,6,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,12,16,18	2,6,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,12,17,18	2,6,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,12,16	2,6,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,12,14,18	2,6,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,12,14,16,17	2,6,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,12,14	2,6,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,12,14,16,17,18	2,6,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,12,17,18	2,6,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,12,16	2,6,13	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,12,17	2,6,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,12,16,18	2,6,13,15,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,12,14	2,6,13	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,12,14,16,17,18	2,6,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,12,14,18	2,6,13,15,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,12,14,16,17	2,6,13,15,17	$2^{-17.5}$

Table 0.1570 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1	2,6,11	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,16,17,18	2,6,11,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,18	2,6,11,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,16,17	2,6,11,15,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,14,17,18	2,6,11,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,14,16	2,6,11	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,14,17	2,6,11,15,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,14,16,18	2,6,11,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,18	2,6,11,13,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,16,17	2,6,11,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1	2,6,11,13,15	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,16,17,18	2,6,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,14,17	2,6,11,13,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,14,16,18	2,6,11,13,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,14,17,18	2,6,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,14,16	2,6,11,13,15	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,12,17,18	2,6,11,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,12,16	2,6,11	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,12,17	2,6,11,15,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,12,16,18	2,6,11,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,12,14	2,6,11	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,12,14,16,17,18	2,6,11,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,12,14,18	2,6,11,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,12,14,16,17	2,6,11,15,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,12,17	2,6,11,13,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,12,16,18	2,6,11,13,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,12,17,18	2,6,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,12,16	2,6,11,13,15	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,12,14,18	2,6,11,13,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,12,14,16,17	2,6,11,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,12,14	2,6,11,13,15	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,12,14,16,17,18	2,6,11,13,15,17,18	$2^{-17.5}$

Table 0.1571 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(2)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,10,17	2,6,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,10,16,18	2,6,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,10,17,18	2,6,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,10,16	2,6,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,10,14,18	2,6,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,10,14,16,17	2,6,17	2^{-34}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,10,14	2,6,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,10,14,16,17,18	2,6,15,17,18	2^{-34}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,10,17,18	2,6,13,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,10,16	2,6,13	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,10,17	2,6,13,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,10,16,18	2,6,13,15,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,10,14	2,6,13	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,10,14,16,17,18	2,6,13,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,10,14,18	2,6,13,15,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,10,14,16,17	2,6,13,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,10,12,18	2,6,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,10,12,16,17	2,6,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,10,12	2,6,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,10,12,16,17,18	2,6,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,10,12,14,17	2,6,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,10,12,14,16,18	2,6,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,10,12,14,17,18	2,6,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,10,12,14,16	2,6,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,10,12	2,6,13	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,10,12,16,17,18	2,6,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,10,12,18	2,6,13,15,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,10,12,16,17	2,6,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,10,12,14,17,18	2,6,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,10,12,14,16	2,6,13	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,10,12,14,17	2,6,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,10,12,14,16,18	2,6,13,15,18	2^{-23}

Table 0.1572 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,10,17,18	2,6,11,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,10,16	2,6,11	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,10,17	2,6,11,15,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,10,16,18	2,6,11,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,10,14	2,6,11	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,10,14,16,17,18	2,6,11,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,10,14,18	2,6,11,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,10,14,16,17	2,6,11,15,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,10,17	2,6,11,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,10,16,18	2,6,11,13,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,10,17,18	2,6,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,10,16	2,6,11,13,15	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,10,14,18	2,6,11,13,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,10,14,16,17	2,6,11,13,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,10,14	2,6,11,13,15	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,10,14,16,17,18	2,6,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,10,12	2,6,11	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,10,12,16,17,18	2,6,11,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,10,12,18	2,6,11,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,10,12,16,17	2,6,11,15,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,10,12,14,17,18	2,6,11,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,10,12,14,16	2,6,11	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,10,12,14,17	2,6,11,15,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,10,12,14,16,18	2,6,11,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,10,12,18	2,6,11,13,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,10,12,16,17	2,6,11,13,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,10,12	2,6,11,13,15	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,10,12,16,17,18	2,6,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,10,12,14,17	2,6,11,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,10,12,14,16,18	2,6,11,13,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,10,12,14,17,18	2,6,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,10,12,14,16	2,6,11,13,15	2^{-23}

Table 0.1573 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1	2,6,9	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,16,17,18	2,6,9,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,18	2,6,9,15,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0)$	1,16,17	2,6,9,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,14,17,18	2,6,9,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,14,16	2,6,9	2^{-34}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,14,17	2,6,9,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,14,16,18	2,6,9,15,18	2^{-34}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,18	2,6,9,13,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,16,17	2,6,9,13,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1	2,6,9,13,15	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,16,17,18	2,6,9,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,14,17	2,6,9,13,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,14,16,18	2,6,9,13,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,14,17,18	2,6,9,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,14,16	2,6,9,13,15	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,12,17,18	2,6,9,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,12,16	2,6,9	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,12,17	2,6,9,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,12,16,18	2,6,9,15,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,12,14	2,6,9	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,12,14,16,17,18	2,6,9,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,12,14,18	2,6,9,15,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,12,14,16,17	2,6,9,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,12,17	2,6,9,13,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,12,16,18	2,6,9,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,12,17,18	2,6,9,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,12,16	2,6,9,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,12,14,18	2,6,9,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,12,14,16,17	2,6,9,13,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,12,14	2,6,9,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,12,14,16,17,18	2,6,9,13,15,17,18	2^{-23}

Table 0.1574 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,18	2,6,9,11,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,16,17	2,6,9,11,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1	2,6,9,11,15	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,16,17,18	2,6,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,14,17	2,6,9,11,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,14,16,18	2,6,9,11,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,14,17,18	2,6,9,11,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,14,16	2,6,9,11,15	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1	2,6,9,11,13	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,16,17,18	2,6,9,11,13,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,18	2,6,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,16,17	2,6,9,11,13,15,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,14,17,18	2,6,9,11,13,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,14,16	2,6,9,11,13	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,14,17	2,6,9,11,13,15,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,14,16,18	2,6,9,11,13,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,12,17	2,6,9,11,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,12,16,18	2,6,9,11,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,12,17,18	2,6,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,12,16	2,6,9,11,15	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,12,14,18	2,6,9,11,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,12,14,16,17	2,6,9,11,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,12,14	2,6,9,11,15	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,12,14,16,17,18	2,6,9,11,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,12,17,18	2,6,9,11,13,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,12,16	2,6,9,11,13	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,12,17	2,6,9,11,13,15,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,12,16,18	2,6,9,11,13,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,12,14	2,6,9,11,13	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,12,14,16,17,18	2,6,9,11,13,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,12,14,18	2,6,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,12,14,16,17	2,6,9,11,13,15,17	2^{-23}

Table 0.1575 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,10,17,18	2,6,9,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,10,16	2,6,9	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,10,17	2,6,9,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,10,16,18	2,6,9,15,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,10,14	2,6,9	2^{-1}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,10,14,16,17,18	2,6,9,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,10,14,18	2,6,9,15,18	2^{-1}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,10,14,16,17	2,6,9,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,10,17	2,6,9,13,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,10,16,18	2,6,9,13,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,10,17,18	2,6,9,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,10,16	2,6,9,13,15	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,10,14,18	2,6,9,13,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,10,14,16,17	2,6,9,13,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,10,14	2,6,9,13,15	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,10,14,16,17,18	2,6,9,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,10,12	2,6,9	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,10,12,16,17,18	2,6,9,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,10,12,18	2,6,9,15,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,10,12,16,17	2,6,9,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,10,12,14,17,18	2,6,9,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,10,12,14,16	2,6,9	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,10,12,14,17	2,6,9,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,10,12,14,16,18	2,6,9,15,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,10,12,18	2,6,9,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,10,12,16,17	2,6,9,13,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,10,12	2,6,9,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,10,12,16,17,18	2,6,9,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,10,12,14,17	2,6,9,13,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,10,12,14,16,18	2,6,9,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,10,12,14,17,18	2,6,9,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,10,12,14,16	2,6,9,13,15	$2^{-17.5}$

Table 0.1576 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,10,17	2,6,9,11,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,10,16,18	2,6,9,11,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,10,17,18	2,6,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,10,16	2,6,9,11,15	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,10,14,18	2,6,9,11,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,10,14,16,17	2,6,9,11,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,10,14	2,6,9,11,15	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,10,14,16,17,18	2,6,9,11,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,10,17,18	2,6,9,11,13,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,10,16	2,6,9,11,13	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,10,17	2,6,9,11,13,15,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,10,16,18	2,6,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,10,14	2,6,9,11,13	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,10,14,16,17,18	2,6,9,11,13,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,10,14,18	2,6,9,11,13,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,10,14,16,17	2,6,9,11,13,15,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,10,12,18	2,6,9,11,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,10,12,16,17	2,6,9,11,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,10,12	2,6,9,11,15	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,10,12,16,17,18	2,6,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,10,12,14,17	2,6,9,11,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,10,12,14,16,18	2,6,9,11,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,10,12,14,17,18	2,6,9,11,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,10,12,14,16	2,6,9,11,15	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,10,12	2,6,9,11,13	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,10,12,16,17,18	2,6,9,11,13,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,10,12,18	2,6,9,11,13,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,10,12,16,17	2,6,9,11,13,15,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,10,12,14,17,18	2,6,9,11,13,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,10,12,14,16	2,6,9,11,13	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,10,12,14,17	2,6,9,11,13,15,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,10,12,14,16,18	2,6,9,11,13,15,18	$2^{-17.5}$

Table 0.1577 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,17	2,6,8,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,16,18	2,6,8,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,17,18	2,6,8,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,16	2,6,8,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,14,18	2,6,8,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,14,16,17	2,6,8,17	2^{-1}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,14	2,6,8,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,14,16,17,18	2,6,8,15,17,18	2^{-1}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,17,18	2,6,8,13,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,16	2,6,8,13	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,17	2,6,8,13,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,16,18	2,6,8,13,15,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,14	2,6,8,13	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,14,16,17,18	2,6,8,13,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,14,18	2,6,8,13,15,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,14,16,17	2,6,8,13,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,12,18	2,6,8,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,12,16,17	2,6,8,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,12	2,6,8,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,12,16,17,18	2,6,8,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,12,14,17	2,6,8,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,12,14,16,18	2,6,8,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,12,14,17,18	2,6,8,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,12,14,16	2,6,8,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,12	2,6,8,13	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,12,16,17,18	2,6,8,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,12,18	2,6,8,13,15,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,12,16,17	2,6,8,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,12,14,17,18	2,6,8,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,12,14,16	2,6,8,13	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,12,14,17	2,6,8,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,12,14,16,18	2,6,8,13,15,18	2^{-12}

Table 0.1578 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,17,18	2,6,8,11,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,16	2,6,8,11	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,17	2,6,8,11,15,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,16,18	2,6,8,11,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,14	2,6,8,11	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,14,16,17,18	2,6,8,11,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,14,18	2,6,8,11,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,14,16,17	2,6,8,11,15,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,17	2,6,8,11,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,16,18	2,6,8,11,13,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,17,18	2,6,8,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,16	2,6,8,11,13,15	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,14,18	2,6,8,11,13,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,14,16,17	2,6,8,11,13,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,14	2,6,8,11,13,15	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,14,16,17,18	2,6,8,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,12	2,6,8,11	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,12,16,17,18	2,6,8,11,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,12,18	2,6,8,11,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,12,16,17	2,6,8,11,15,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,12,14,17,18	2,6,8,11,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,12,14,16	2,6,8,11	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,12,14,17	2,6,8,11,15,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,12,14,16,18	2,6,8,11,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,12,18	2,6,8,11,13,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,12,16,17	2,6,8,11,13,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,12	2,6,8,11,13,15	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,12,16,17,18	2,6,8,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,12,14,17	2,6,8,11,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,12,14,16,18	2,6,8,11,13,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,12,14,17,18	2,6,8,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,12,14,16	2,6,8,11,13,15	2^{-12}

Table 0.1579 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,10,18	2,6,8,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,10,16,17	2,6,8,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,10	2,6,8,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,10,16,17,18	2,6,8,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,10,14,17	2,6,8,17	2^{-34}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,10,14,16,18	2,6,8,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,10,14,17,18	2,6,8,15,17,18	2^{-34}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,10,14,16	2,6,8,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,10	2,6,8,13	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,10,16,17,18	2,6,8,13,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,10,18	2,6,8,13,15,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,10,16,17	2,6,8,13,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,10,14,17,18	2,6,8,13,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,10,14,16	2,6,8,13	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,10,14,17	2,6,8,13,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,10,14,16,18	2,6,8,13,15,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,10,12,17	2,6,8,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,10,12,16,18	2,6,8,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,10,12,17,18	2,6,8,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,10,12,16	2,6,8,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,10,12,14,18	2,6,8,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,10,12,14,16,17	2,6,8,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,10,12,14	2,6,8,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,10,12,14,16,17,18	2,6,8,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,10,12,17,18	2,6,8,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,10,12,16	2,6,8,13	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,10,12,17	2,6,8,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,10,12,16,18	2,6,8,13,15,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,10,12,14	2,6,8,13	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,10,12,14,16,17,18	2,6,8,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,10,12,14,18	2,6,8,13,15,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,10,12,14,16,17	2,6,8,13,15,17	$2^{-17.5}$

Table 0.1580 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,10	2,6,8,11	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,10,16,17,18	2,6,8,11,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,10,18	2,6,8,11,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,10,16,17	2,6,8,11,15,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,10,14,17,18	2,6,8,11,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,10,14,16	2,6,8,11	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,10,14,17	2,6,8,11,15,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,10,14,16,18	2,6,8,11,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,10,18	2,6,8,11,13,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,10,16,17	2,6,8,11,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,10	2,6,8,11,13,15	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,10,16,17,18	2,6,8,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,10,14,17	2,6,8,11,13,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,10,14,16,18	2,6,8,11,13,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,10,14,17,18	2,6,8,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,10,14,16	2,6,8,11,13,15	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,10,12,17,18	2,6,8,11,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,10,12,16	2,6,8,11	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,10,12,17	2,6,8,11,15,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,10,12,16,18	2,6,8,11,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,10,12,14	2,6,8,11	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,10,12,14,16,17,18	2,6,8,11,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,10,12,14,18	2,6,8,11,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,10,12,14,16,17	2,6,8,11,15,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,10,12,17	2,6,8,11,13,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,10,12,16,18	2,6,8,11,13,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,10,12,17,18	2,6,8,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,10,12,16	2,6,8,11,13,15	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,10,12,14,18	2,6,8,11,13,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,10,12,14,16,17	2,6,8,11,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,10,12,14	2,6,8,11,13,15	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,10,12,14,16,17,18	2,6,8,11,13,15,17,18	$2^{-17.5}$

Table 0.1581 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,17,18	2,6,8,9,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,16	2,6,8,9	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,17	2,6,8,9,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,16,18	2,6,8,9,15,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,14	2,6,8,9	2^{-34}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,14,16,17,18	2,6,8,9,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,14,18	2,6,8,9,15,18	2^{-34}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,14,16,17	2,6,8,9,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,17	2,6,8,9,13,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,16,18	2,6,8,9,13,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,17,18	2,6,8,9,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,16	2,6,8,9,13,15	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,14,18	2,6,8,9,13,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,14,16,17	2,6,8,9,13,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,14	2,6,8,9,13,15	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,14,16,17,18	2,6,8,9,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,12	2,6,8,9	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,12,16,17,18	2,6,8,9,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,12,18	2,6,8,9,15,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,12,16,17	2,6,8,9,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,12,14,17,18	2,6,8,9,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,12,14,16	2,6,8,9	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,12,14,17	2,6,8,9,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,12,14,16,18	2,6,8,9,15,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,12,18	2,6,8,9,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,12,16,17	2,6,8,9,13,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,12	2,6,8,9,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,12,16,17,18	2,6,8,9,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,12,14,17	2,6,8,9,13,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,12,14,16,18	2,6,8,9,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,12,14,17,18	2,6,8,9,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,12,14,16	2,6,8,9,13,15	$2^{-17.5}$

Table 0.1582 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,17	2,6,8,9,11,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,16,18	2,6,8,9,11,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,17,18	2,6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,16	2,6,8,9,11,15	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,14,18	2,6,8,9,11,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,14,16,17	2,6,8,9,11,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,14	2,6,8,9,11,15	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,14,16,17,18	2,6,8,9,11,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,17,18	2,6,8,9,11,13,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,16	2,6,8,9,11,13	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,17	2,6,8,9,11,13,15,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,16,18	2,6,8,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,14	2,6,8,9,11,13	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,14,16,17,18	2,6,8,9,11,13,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,14,18	2,6,8,9,11,13,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,14,16,17	2,6,8,9,11,13,15,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,12,18	2,6,8,9,11,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,12,16,17	2,6,8,9,11,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,12	2,6,8,9,11,15	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,12,16,17,18	2,6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,12,14,17	2,6,8,9,11,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,12,14,16,18	2,6,8,9,11,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,12,14,17,18	2,6,8,9,11,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,12,14,16	2,6,8,9,11,15	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,12	2,6,8,9,11,13	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,12,16,17,18	2,6,8,9,11,13,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,12,18	2,6,8,9,11,13,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,12,16,17	2,6,8,9,11,13,15,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,12,14,17,18	2,6,8,9,11,13,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,12,14,16	2,6,8,9,11,13	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,12,14,17	2,6,8,9,11,13,15,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,12,14,16,18	2,6,8,9,11,13,15,18	$2^{-17.5}$

Table 0.1583 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,10	2,6,8,9	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,10,16,17,18	2,6,8,9,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,10,18	2,6,8,9,15,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,10,16,17	2,6,8,9,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,10,14,17,18	2,6,8,9,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,10,14,16	2,6,8,9	2^{-1}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,10,14,17	2,6,8,9,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,10,14,16,18	2,6,8,9,15,18	2^{-1}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,10,18	2,6,8,9,13,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,10,16,17	2,6,8,9,13,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,10	2,6,8,9,13,15	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,10,16,17,18	2,6,8,9,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,10,14,17	2,6,8,9,13,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,10,14,16,18	2,6,8,9,13,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,10,14,17,18	2,6,8,9,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,10,14,16	2,6,8,9,13,15	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,10,12,17,18	2,6,8,9,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,10,12,16	2,6,8,9	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,10,12,17	2,6,8,9,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,10,12,16,18	2,6,8,9,15,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,10,12,14	2,6,8,9	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,10,12,14,16,17,18	2,6,8,9,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,10,12,14,18	2,6,8,9,15,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,10,12,14,16,17	2,6,8,9,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,10,12,17	2,6,8,9,13,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,10,12,16,18	2,6,8,9,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,10,12,17,18	2,6,8,9,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,10,12,16	2,6,8,9,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,10,12,14,18	2,6,8,9,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,10,12,14,16,17	2,6,8,9,13,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,10,12,14	2,6,8,9,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,10,12,14,16,17,18	2,6,8,9,13,15,17,18	2^{-12}

Table 0.1584 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,10,18	2,6,8,9,11,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,10,16,17	2,6,8,9,11,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,10	2,6,8,9,11,15	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,10,16,17,18	2,6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,10,14,17	2,6,8,9,11,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,10,14,16,18	2,6,8,9,11,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,10,14,17,18	2,6,8,9,11,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,10,14,16	2,6,8,9,11,15	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,10	2,6,8,9,11,13	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,10,16,17,18	2,6,8,9,11,13,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,10,18	2,6,8,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,10,16,17	2,6,8,9,11,13,15,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,10,14,17,18	2,6,8,9,11,13,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,10,14,16	2,6,8,9,11,13	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,10,14,17	2,6,8,9,11,13,15,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,10,14,16,18	2,6,8,9,11,13,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,10,12,17	2,6,8,9,11,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,10,12,16,18	2,6,8,9,11,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,10,12,17,18	2,6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,10,12,16	2,6,8,9,11,15	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,10,12,14,18	2,6,8,9,11,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,10,12,14,16,17	2,6,8,9,11,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,10,12,14	2,6,8,9,11,15	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,10,12,14,16,17,18	2,6,8,9,11,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,10,12,17,18	2,6,8,9,11,13,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,10,12,16	2,6,8,9,11,13	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,10,12,17	2,6,8,9,11,13,15,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,10,12,16,18	2,6,8,9,11,13,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,10,12,14	2,6,8,9,11,13	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,10,12,14,16,17,18	2,6,8,9,11,13,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,10,12,14,18	2,6,8,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,10,12,14,16,17	2,6,8,9,11,13,15,17	2^{-12}

Table 0.1585 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,7	2,6	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,7,16,17,18	2,6,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,7,18	2,6,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,7,16,17	2,6,15,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,7,14,17,18	2,6,17,18	2^{-1}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,7,14,16	2,6	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,7,14,17	2,6,15,17	2^{-1}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,7,14,16,18	2,6,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,7,18	2,6,13,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,7,16,17	2,6,13,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,7	2,6,13,15	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,7,16,17,18	2,6,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,7,14,17	2,6,13,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,7,14,16,18	2,6,13,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,7,14,17,18	2,6,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,7,14,16	2,6,13,15	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,7,12,17,18	2,6,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,7,12,16	2,6	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,7,12,17	2,6,15,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,7,12,16,18	2,6,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,7,12,14	2,6	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,7,12,14,16,17,18	2,6,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,7,12,14,18	2,6,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,7,12,14,16,17	2,6,15,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,7,12,17	2,6,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,7,12,16,18	2,6,13,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,7,12,17,18	2,6,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,7,12,16	2,6,13,15	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,7,12,14,18	2,6,13,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,7,12,14,16,17	2,6,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,7,12,14	2,6,13,15	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,7,12,14,16,17,18	2,6,13,15,17,18	$2^{-17.5}$

Table 0.1586 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,7,18	2,6,11,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,7,16,17	2,6,11,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,7	2,6,11,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,7,16,17,18	2,6,11,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,7,14,17	2,6,11,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,7,14,16,18	2,6,11,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,7,14,17,18	2,6,11,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,7,14,16	2,6,11,15	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,7	2,6,11,13	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,7,16,17,18	2,6,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,7,18	2,6,11,13,15,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,7,16,17	2,6,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,7,14,17,18	2,6,11,13,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,7,14,16	2,6,11,13	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,7,14,17	2,6,11,13,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,7,14,16,18	2,6,11,13,15,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,7,12,17	2,6,11,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,7,12,16,18	2,6,11,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,7,12,17,18	2,6,11,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,7,12,16	2,6,11,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,7,12,14,18	2,6,11,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,7,12,14,16,17	2,6,11,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,7,12,14	2,6,11,15	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,7,12,14,16,17,18	2,6,11,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,7,12,17,18	2,6,11,13,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,7,12,16	2,6,11,13	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,7,12,17	2,6,11,13,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,7,12,16,18	2,6,11,13,15,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,7,12,14	2,6,11,13	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,7,12,14,16,17,18	2,6,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,7,12,14,18	2,6,11,13,15,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,7,12,14,16,17	2,6,11,13,15,17	$2^{-17.5}$

Table 0.1587 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,7,10,17,18	2,6,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,7,10,16	2,6	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,7,10,17	2,6,15,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,7,10,16,18	2,6,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,7,10,14	2,6	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,7,10,14,16,17,18	2,6,17,18	2^{-34}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,7,10,14,18	2,6,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,7,10,14,16,17	2,6,15,17	2^{-34}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,7,10,17	2,6,13,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,7,10,16,18	2,6,13,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,7,10,17,18	2,6,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,7,10,16	2,6,13,15	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,7,10,14,18	2,6,13,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,7,10,14,16,17	2,6,13,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,7,10,14	2,6,13,15	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,7,10,14,16,17,18	2,6,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,7,10,12	2,6	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,7,10,12,16,17,18	2,6,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,7,10,12,18	2,6,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,7,10,12,16,17	2,6,15,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,7,10,12,14,17,18	2,6,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1)$	1,7,10,12,14,16	2,6	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,7,10,12,14,17	2,6,15,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,7,10,12,14,16,18	2,6,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,7,10,12,18	2,6,13,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,7,10,12,16,17	2,6,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,7,10,12	2,6,13,15	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,7,10,12,16,17,18	2,6,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,7,10,12,14,17	2,6,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,7,10,12,14,16,18	2,6,13,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,7,10,12,14,17,18	2,6,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,7,10,12,14,16	2,6,13,15	2^{-23}

Table 0.1588 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,7,10,17	2,6,11,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,7,10,16,18	2,6,11,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,7,10,17,18	2,6,11,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,7,10,16	2,6,11,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,7,10,14,18	2,6,11,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,7,10,14,16,17	2,6,11,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,7,10,14	2,6,11,15	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,7,10,14,16,17,18	2,6,11,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,7,10,17,18	2,6,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,7,10,16	2,6,11,13	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,7,10,17	2,6,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,7,10,16,18	2,6,11,13,15,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,7,10,14	2,6,11,13	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,7,10,14,16,17,18	2,6,11,13,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,7,10,14,18	2,6,11,13,15,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,7,10,14,16,17	2,6,11,13,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,7,10,12,18	2,6,11,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,7,10,12,16,17	2,6,11,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,7,10,12	2,6,11,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,7,10,12,16,17,18	2,6,11,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,7,10,12,14,17	2,6,11,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,7,10,12,14,16,18	2,6,11,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,7,10,12,14,17,18	2,6,11,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,7,10,12,14,16	2,6,11,15	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,7,10,12	2,6,11,13	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,7,10,12,16,17,18	2,6,11,13,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,7,10,12,18	2,6,11,13,15,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,7,10,12,16,17	2,6,11,13,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,7,10,12,14,17,18	2,6,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,7,10,12,14,16	2,6,11,13	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,7,10,12,14,17	2,6,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,7,10,12,14,16,18	2,6,11,13,15,18	2^{-23}

Table 0.1589 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,7,18	2,6,9,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,7,16,17	2,6,9,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,7	2,6,9,15	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,7,16,17,18	2,6,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,7,14,17	2,6,9,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,7,14,16,18	2,6,9,18	2^{-34}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,7,14,17,18	2,6,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,7,14,16	2,6,9,15	2^{-34}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,7	2,6,9,13	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,7,16,17,18	2,6,9,13,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,7,18	2,6,9,13,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,7,16,17	2,6,9,13,15,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,7,14,17,18	2,6,9,13,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,7,14,16	2,6,9,13	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,7,14,17	2,6,9,13,15,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,7,14,16,18	2,6,9,13,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,7,12,17	2,6,9,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,7,12,16,18	2,6,9,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,7,12,17,18	2,6,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,7,12,16	2,6,9,15	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,7,12,14,18	2,6,9,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,7,12,14,16,17	2,6,9,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,7,12,14	2,6,9,15	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,7,12,14,16,17,18	2,6,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,7,12,17,18	2,6,9,13,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,7,12,16	2,6,9,13	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,7,12,17	2,6,9,13,15,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,7,12,16,18	2,6,9,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,7,12,14	2,6,9,13	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,7,12,14,16,17,18	2,6,9,13,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,7,12,14,18	2,6,9,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,7,12,14,16,17	2,6,9,13,15,17	2^{-23}

Table 0.1590 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,7	2,6,9,11	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,7,16,17,18	2,6,9,11,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,7,18	2,6,9,11,15,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,7,16,17	2,6,9,11,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,7,14,17,18	2,6,9,11,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,7,14,16	2,6,9,11	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,7,14,17	2,6,9,11,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,7,14,16,18	2,6,9,11,15,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,7,18	2,6,9,11,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,7,16,17	2,6,9,11,13,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,7	2,6,9,11,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,7,16,17,18	2,6,9,11,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,7,14,17	2,6,9,11,13,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,7,14,16,18	2,6,9,11,13,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,7,14,17,18	2,6,9,11,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,7,14,16	2,6,9,11,13,15	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,7,12,17,18	2,6,9,11,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,7,12,16	2,6,9,11	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,7,12,17	2,6,9,11,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,7,12,16,18	2,6,9,11,15,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,7,12,14	2,6,9,11	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,7,12,14,16,17,18	2,6,9,11,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,7,12,14,18	2,6,9,11,15,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,7,12,14,16,17	2,6,9,11,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,7,12,17	2,6,9,11,13,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,7,12,16,18	2,6,9,11,13,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,7,12,17,18	2,6,9,11,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,7,12,16	2,6,9,11,13,15	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,7,12,14,18	2,6,9,11,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,7,12,14,16,17	2,6,9,11,13,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,7,12,14	2,6,9,11,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,7,12,14,16,17,18	2,6,9,11,13,15,17,18	2^{-23}

Table 0.1591 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,7,10,17	2,6,9,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,7,10,16,18	2,6,9,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,7,10,17,18	2,6,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,7,10,16	2,6,9,15	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,7,10,14,18	2,6,9,18	2^{-1}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,7,10,14,16,17	2,6,9,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,7,10,14	2,6,9,15	2^{-1}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,7,10,14,16,17,18	2,6,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,7,10,17,18	2,6,9,13,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,7,10,16	2,6,9,13	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,7,10,17	2,6,9,13,15,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,7,10,16,18	2,6,9,13,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,7,10,14	2,6,9,13	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,7,10,14,16,17,18	2,6,9,13,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,7,10,14,18	2,6,9,13,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,7,10,14,16,17	2,6,9,13,15,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,7,10,12,18	2,6,9,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,7,10,12,16,17	2,6,9,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,7,10,12	2,6,9,15	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,7,10,12,16,17,18	2,6,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,7,10,12,14,17	2,6,9,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,7,10,12,14,16,18	2,6,9,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,7,10,12,14,17,18	2,6,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,7,10,12,14,16	2,6,9,15	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,7,10,12	2,6,9,13	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,7,10,12,16,17,18	2,6,9,13,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,7,10,12,18	2,6,9,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,7,10,12,16,17	2,6,9,13,15,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,7,10,12,14,17,18	2,6,9,13,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,7,10,12,14,16	2,6,9,13	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,7,10,12,14,17	2,6,9,13,15,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,7,10,12,14,16,18	2,6,9,13,15,18	$2^{-17.5}$

Table 0.1592 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,7,10,17,18	2,6,9,11,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,7,10,16	2,6,9,11	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,7,10,17	2,6,9,11,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,7,10,16,18	2,6,9,11,15,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,7,10,14	2,6,9,11	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,7,10,14,16,17,18	2,6,9,11,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,7,10,14,18	2,6,9,11,15,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,7,10,14,16,17	2,6,9,11,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,7,10,17	2,6,9,11,13,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,7,10,16,18	2,6,9,11,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,7,10,17,18	2,6,9,11,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,7,10,16	2,6,9,11,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,7,10,14,18	2,6,9,11,13,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,7,10,14,16,17	2,6,9,11,13,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,7,10,14	2,6,9,11,13,15	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,7,10,14,16,17,18	2,6,9,11,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,7,10,12	2,6,9,11	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,7,10,12,16,17,18	2,6,9,11,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,7,10,12,18	2,6,9,11,15,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,7,10,12,16,17	2,6,9,11,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,7,10,12,14,17,18	2,6,9,11,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,7,10,12,14,16	2,6,9,11	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,7,10,12,14,17	2,6,9,11,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,7,10,12,14,16,18	2,6,9,11,15,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,7,10,12,18	2,6,9,11,13,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,7,10,12,16,17	2,6,9,11,13,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,7,10,12	2,6,9,11,13,15	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,7,10,12,16,17,18	2,6,9,11,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,7,10,12,14,17	2,6,9,11,13,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,7,10,12,14,16,18	2,6,9,11,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,7,10,12,14,17,18	2,6,9,11,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,7,10,12,14,16	2,6,9,11,13,15	$2^{-17.5}$

Table 0.1593 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,7,17,18	2,6,8,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,7,16	2,6,8	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,7,17	2,6,8,15,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,7,16,18	2,6,8,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,7,14	2,6,8	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,7,14,16,17,18	2,6,8,17,18	2^{-1}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,7,14,18	2,6,8,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,7,14,16,17	2,6,8,15,17	2^{-1}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,7,17	2,6,8,13,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,7,16,18	2,6,8,13,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,7,17,18	2,6,8,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,7,16	2,6,8,13,15	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,7,14,18	2,6,8,13,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,7,14,16,17	2,6,8,13,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,7,14	2,6,8,13,15	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,7,14,16,17,18	2,6,8,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,7,12	2,6,8	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,7,12,16,17,18	2,6,8,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,7,12,18	2,6,8,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,7,12,16,17	2,6,8,15,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,7,12,14,17,18	2,6,8,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,7,12,14,16	2,6,8	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,7,12,14,17	2,6,8,15,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,7,12,14,16,18	2,6,8,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,7,12,18	2,6,8,13,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,7,12,16,17	2,6,8,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,7,12	2,6,8,13,15	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,7,12,16,17,18	2,6,8,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,7,12,14,17	2,6,8,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,7,12,14,16,18	2,6,8,13,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,7,12,14,17,18	2,6,8,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,7,12,14,16	2,6,8,13,15	2^{-12}

Table 0.1594 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,7,17	2,6,8,11,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,7,16,18	2,6,8,11,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,7,17,18	2,6,8,11,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,7,16	2,6,8,11,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,7,14,18	2,6,8,11,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,7,14,16,17	2,6,8,11,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,7,14	2,6,8,11,15	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,7,14,16,17,18	2,6,8,11,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,7,17,18	2,6,8,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,7,16	2,6,8,11,13	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,7,17	2,6,8,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,7,16,18	2,6,8,11,13,15,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,7,14	2,6,8,11,13	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,7,14,16,17,18	2,6,8,11,13,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,7,14,18	2,6,8,11,13,15,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,7,14,16,17	2,6,8,11,13,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,7,12,18	2,6,8,11,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,7,12,16,17	2,6,8,11,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,7,12	2,6,8,11,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,7,12,16,17,18	2,6,8,11,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,7,12,14,17	2,6,8,11,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,7,12,14,16,18	2,6,8,11,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,7,12,14,17,18	2,6,8,11,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,7,12,14,16	2,6,8,11,15	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,7,12	2,6,8,11,13	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,7,12,16,17,18	2,6,8,11,13,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,7,12,18	2,6,8,11,13,15,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,7,12,16,17	2,6,8,11,13,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,7,12,14,17,18	2,6,8,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,7,12,14,16	2,6,8,11,13	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,7,12,14,17	2,6,8,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,7,12,14,16,18	2,6,8,11,13,15,18	2^{-12}

Table 0.1595 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,7,10	2,6,8	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,7,10,16,17,18	2,6,8,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,7,10,18	2,6,8,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,7,10,16,17	2,6,8,15,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,7,10,14,17,18	2,6,8,17,18	2^{-34}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,7,10,14,16	2,6,8	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,7,10,14,17	2,6,8,15,17	2^{-34}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,7,10,14,16,18	2,6,8,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,7,10,18	2,6,8,13,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,7,10,16,17	2,6,8,13,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,7,10	2,6,8,13,15	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,7,10,16,17,18	2,6,8,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,7,10,14,17	2,6,8,13,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,7,10,14,16,18	2,6,8,13,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,7,10,14,17,18	2,6,8,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,7,10,14,16	2,6,8,13,15	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,7,10,12,17,18	2,6,8,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,7,10,12,16	2,6,8	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,7,10,12,17	2,6,8,15,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,7,10,12,16,18	2,6,8,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,7,10,12,14	2,6,8	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,7,10,12,14,16,17,18	2,6,8,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,7,10,12,14,18	2,6,8,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,7,10,12,14,16,17	2,6,8,15,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,7,10,12,17	2,6,8,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,7,10,12,16,18	2,6,8,13,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,7,10,12,17,18	2,6,8,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,7,10,12,16	2,6,8,13,15	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,7,10,12,14,18	2,6,8,13,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,7,10,12,14,16,17	2,6,8,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,7,10,12,14	2,6,8,13,15	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,7,10,12,14,16,17,18	2,6,8,13,15,17,18	$2^{-17.5}$

Table 0.1596 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,7,10,18	2,6,8,11,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,7,10,16,17	2,6,8,11,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,7,10	2,6,8,11,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,7,10,16,17,18	2,6,8,11,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,7,10,14,17	2,6,8,11,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,7,10,14,16,18	2,6,8,11,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,7,10,14,17,18	2,6,8,11,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,7,10,14,16	2,6,8,11,15	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,7,10	2,6,8,11,13	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,7,10,16,17,18	2,6,8,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,7,10,18	2,6,8,11,13,15,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,7,10,16,17	2,6,8,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,7,10,14,17,18	2,6,8,11,13,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,7,10,14,16	2,6,8,11,13	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,7,10,14,17	2,6,8,11,13,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,7,10,14,16,18	2,6,8,11,13,15,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,7,10,12,17	2,6,8,11,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,7,10,12,16,18	2,6,8,11,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,7,10,12,17,18	2,6,8,11,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,7,10,12,16	2,6,8,11,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,7,10,12,14,18	2,6,8,11,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,7,10,12,14,16,17	2,6,8,11,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,7,10,12,14	2,6,8,11,15	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,7,10,12,14,16,17,18	2,6,8,11,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,7,10,12,17,18	2,6,8,11,13,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,7,10,12,16	2,6,8,11,13	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,7,10,12,17	2,6,8,11,13,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,7,10,12,16,18	2,6,8,11,13,15,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,7,10,12,14	2,6,8,11,13	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,7,10,12,14,16,17,18	2,6,8,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,7,10,12,14,18	2,6,8,11,13,15,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,7,10,12,14,16,17	2,6,8,11,13,15,17	$2^{-17.5}$

Table 0.1597 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,7,17	2,6,8,9,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,7,16,18	2,6,8,9,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,7,17,18	2,6,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,7,16	2,6,8,9,15	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,7,14,18	2,6,8,9,18	2^{-34}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,7,14,16,17	2,6,8,9,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,7,14	2,6,8,9,15	2^{-34}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,7,14,16,17,18	2,6,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,7,17,18	2,6,8,9,13,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,7,16	2,6,8,9,13	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,7,17	2,6,8,9,13,15,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,7,16,18	2,6,8,9,13,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,7,14	2,6,8,9,13	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,7,14,16,17,18	2,6,8,9,13,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,7,14,18	2,6,8,9,13,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,7,14,16,17	2,6,8,9,13,15,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,7,12,18	2,6,8,9,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,7,12,16,17	2,6,8,9,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,7,12	2,6,8,9,15	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,7,12,16,17,18	2,6,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,7,12,14,17	2,6,8,9,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,7,12,14,16,18	2,6,8,9,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,7,12,14,17,18	2,6,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,7,12,14,16	2,6,8,9,15	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,7,12	2,6,8,9,13	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,7,12,16,17,18	2,6,8,9,13,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,7,12,18	2,6,8,9,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,7,12,16,17	2,6,8,9,13,15,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,7,12,14,17,18	2,6,8,9,13,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,7,12,14,16	2,6,8,9,13	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,7,12,14,17	2,6,8,9,13,15,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,7,12,14,16,18	2,6,8,9,13,15,18	$2^{-17.5}$

Table 0.1598 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,7,17,18	2,6,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,7,16	2,6,8,9,11	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,7,17	2,6,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,7,16,18	2,6,8,9,11,15,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,7,14	2,6,8,9,11	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,7,14,16,17,18	2,6,8,9,11,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,7,14,18	2,6,8,9,11,15,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,7,14,16,17	2,6,8,9,11,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,7,17	2,6,8,9,11,13,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,7,16,18	2,6,8,9,11,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,7,17,18	2,6,8,9,11,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,7,16	2,6,8,9,11,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,7,14,18	2,6,8,9,11,13,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,7,14,16,17	2,6,8,9,11,13,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,7,14	2,6,8,9,11,13,15	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,7,14,16,17,18	2,6,8,9,11,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,7,12	2,6,8,9,11	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,7,12,16,17,18	2,6,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,7,12,18	2,6,8,9,11,15,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,7,12,16,17	2,6,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,7,12,14,17,18	2,6,8,9,11,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,7,12,14,16	2,6,8,9,11	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,7,12,14,17	2,6,8,9,11,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,7,12,14,16,18	2,6,8,9,11,15,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,7,12,18	2,6,8,9,11,13,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,7,12,16,17	2,6,8,9,11,13,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,7,12	2,6,8,9,11,13,15	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,7,12,16,17,18	2,6,8,9,11,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,7,12,14,17	2,6,8,9,11,13,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,7,12,14,16,18	2,6,8,9,11,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,7,12,14,17,18	2,6,8,9,11,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,7,12,14,16	2,6,8,9,11,13,15	$2^{-17.5}$

Table 0.1599 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,7,10,18	2,6,8,9,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,7,10,16,17	2,6,8,9,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,7,10	2,6,8,9,15	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,7,10,16,17,18	2,6,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,7,10,14,17	2,6,8,9,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,7,10,14,16,18	2,6,8,9,18	2^{-1}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,7,10,14,17,18	2,6,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,7,10,14,16	2,6,8,9,15	2^{-1}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,7,10	2,6,8,9,13	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,7,10,16,17,18	2,6,8,9,13,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,7,10,18	2,6,8,9,13,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,7,10,16,17	2,6,8,9,13,15,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,7,10,14,17,18	2,6,8,9,13,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,7,10,14,16	2,6,8,9,13	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,7,10,14,17	2,6,8,9,13,15,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,7,10,14,16,18	2,6,8,9,13,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,7,10,12,17	2,6,8,9,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,7,10,12,16,18	2,6,8,9,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,7,10,12,17,18	2,6,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,7,10,12,16	2,6,8,9,15	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,7,10,12,14,18	2,6,8,9,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,7,10,12,14,16,17	2,6,8,9,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,7,10,12,14	2,6,8,9,15	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,7,10,12,14,16,17,18	2,6,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,7,10,12,17,18	2,6,8,9,13,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,7,10,12,16	2,6,8,9,13	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,7,10,12,17	2,6,8,9,13,15,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,7,10,12,16,18	2,6,8,9,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,7,10,12,14	2,6,8,9,13	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,7,10,12,14,16,17,18	2,6,8,9,13,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,7,10,12,14,18	2,6,8,9,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,7,10,12,14,16,17	2,6,8,9,13,15,17	2^{-12}

Table 0.1600 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,7,10	2,6,8,9,11	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,7,10,16,17,18	2,6,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,7,10,18	2,6,8,9,11,15,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,7,10,16,17	2,6,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,7,10,14,17,18	2,6,8,9,11,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,7,10,14,16	2,6,8,9,11	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,7,10,14,17	2,6,8,9,11,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,7,10,14,16,18	2,6,8,9,11,15,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,7,10,18	2,6,8,9,11,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,7,10,16,17	2,6,8,9,11,13,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,7,10	2,6,8,9,11,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,7,10,16,17,18	2,6,8,9,11,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,7,10,14,17	2,6,8,9,11,13,17	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,7,10,14,16,18	2,6,8,9,11,13,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,7,10,14,17,18	2,6,8,9,11,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,7,10,14,16	2,6,8,9,11,13,15	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,7,10,12,17,18	2,6,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,7,10,12,16	2,6,8,9,11	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,7,10,12,17	2,6,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,7,10,12,16,18	2,6,8,9,11,15,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,7,10,12,14	2,6,8,9,11	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,7,10,12,14,16,17,18	2,6,8,9,11,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,7,10,12,14,18	2,6,8,9,11,15,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,7,10,12,14,16,17	2,6,8,9,11,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,7,10,12,17	2,6,8,9,11,13,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,7,10,12,16,18	2,6,8,9,11,13,18	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,7,10,12,17,18	2,6,8,9,11,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,7,10,12,16	2,6,8,9,11,13,15	$2^{-6.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,7,10,12,14,18	2,6,8,9,11,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,7,10,12,14,16,17	2,6,8,9,11,13,17	2^{-12}
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,7,10,12,14	2,6,8,9,11,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,7,10,12,14,16,17,18	2,6,8,9,11,13,15,17,18	2^{-12}

Table 0.1601 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,5,17,18	2,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,5,16	2	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1)$	1,5,17	2,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,5,16,18	2,15,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,5,14	2	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,14,16,17,18	2,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,5,14,18	2,15,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,14,16,17	2,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,5,17	2,13,17	2^{-1}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,5,16,18	2,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,5,17,18	2,13,15,17,18	2^{-1}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,5,16	2,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,5,14,18	2,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,5,14,16,17	2,13,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,5,14	2,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,5,14,16,17,18	2,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,12	2	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,5,12,16,17,18	2,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,5,12,18	2,15,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,5,12,16,17	2,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,5,12,14,17,18	2,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,5,12,14,16	2	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,5,12,14,17	2,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,5,12,14,16,18	2,15,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,5,12,18	2,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,12,16,17	2,13,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,5,12	2,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,5,12,16,17,18	2,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,5,12,14,17	2,13,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,5,12,14,16,18	2,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,5,12,14,17,18	2,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,5,12,14,16	2,13,15	$2^{-17.5}$

Table 0.1602 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,5,17	2,11,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,5,16,18	2,11,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,5,17,18	2,11,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,5,16	2,11,15	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,5,14,18	2,11,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,14,16,17	2,11,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,5,14	2,11,15	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,14,16,17,18	2,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,17,18	2,11,13,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,5,16	2,11,13	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,17	2,11,13,15,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,5,16,18	2,11,13,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,5,14	2,11,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,5,14,16,17,18	2,11,13,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,5,14,18	2,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,5,14,16,17	2,11,13,15,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,5,12,18	2,11,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,5,12,16,17	2,11,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,5,12	2,11,15	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,5,12,16,17,18	2,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,5,12,14,17	2,11,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,5,12,14,16,18	2,11,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,5,12,14,17,18	2,11,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,5,12,14,16	2,11,15	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,5,12	2,11,13	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,5,12,16,17,18	2,11,13,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,5,12,18	2,11,13,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,5,12,16,17	2,11,13,15,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,5,12,14,17,18	2,11,13,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,5,12,14,16	2,11,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,5,12,14,17	2,11,13,15,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,5,12,14,16,18	2,11,13,15,18	$2^{-17.5}$

Table 0.1603 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,5,10	2	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,5,10,16,17,18	2,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,5,10,18	2,15,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,5,10,16,17	2,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,5,10,14,17,18	2,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,5,10,14,16	2	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,5,10,14,17	2,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,5,10,14,16,18	2,15,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,5,10,18	2,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,5,10,16,17	2,13,17	2^{-34}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,5,10	2,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,5,10,16,17,18	2,13,15,17,18	2^{-34}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,5,10,14,17	2,13,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,5,10,14,16,18	2,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,5,10,14,17,18	2,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,5,10,14,16	2,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,5,10,12,17,18	2,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,5,10,12,16	2	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,5,10,12,17	2,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,5,10,12,16,18	2,15,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,5,10,12,14	2	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,5,10,12,14,16,17,18	2,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,5,10,12,14,18	2,15,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,5,10,12,14,16,17	2,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,5,10,12,17	2,13,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,5,10,12,16,18	2,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,5,10,12,17,18	2,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,5,10,12,16	2,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,5,10,12,14,18	2,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,5,10,12,14,16,17	2,13,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,5,10,12,14	2,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,5,10,12,14,16,17,18	2,13,15,17,18	2^{-23}

Table 0.1604 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,5,10,18	2,11,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,5,10,16,17	2,11,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,5,10	2,11,15	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,5,10,16,17,18	2,11,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,5,10,14,17	2,11,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,5,10,14,16,18	2,11,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,5,10,14,17,18	2,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,5,10,14,16	2,11,15	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,5,10	2,11,13	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,5,10,16,17,18	2,11,13,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,5,10,18	2,11,13,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,5,10,16,17	2,11,13,15,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,5,10,14,17,18	2,11,13,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,5,10,14,16	2,11,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,5,10,14,17	2,11,13,15,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,5,10,14,16,18	2,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,5,10,12,17	2,11,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,5,10,12,16,18	2,11,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,5,10,12,17,18	2,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,5,10,12,16	2,11,15	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,5,10,12,14,18	2,11,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,5,10,12,14,16,17	2,11,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,5,10,12,14	2,11,15	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,5,10,12,14,16,17,18	2,11,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,5,10,12,17,18	2,11,13,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,5,10,12,16	2,11,13	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,5,10,12,17	2,11,13,15,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,5,10,12,16,18	2,11,13,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,5,10,12,14	2,11,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,5,10,12,14,16,17,18	2,11,13,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,5,10,12,14,18	2,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,5,10,12,14,16,17	2,11,13,15,17	2^{-23}

Table 0.1605 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,17	2,9,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,5,16,18	2,9,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,5,17,18	2,9,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,5,16	2,9,15	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,5,14,18	2,9,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,5,14,16,17	2,9,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,5,14	2,9,15	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,5,14,16,17,18	2,9,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,17,18	2,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,5,16	2,9,13	2^{-34}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,17	2,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,5,16,18	2,9,13,15,18	2^{-34}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1,5,14	2,9,13	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,14,16,17,18	2,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,5,14,18	2,9,13,15,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,14,16,17	2,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,5,12,18	2,9,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,5,12,16,17	2,9,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,5,12	2,9,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,5,12,16,17,18	2,9,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,5,12,14,17	2,9,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,5,12,14,16,18	2,9,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,5,12,14,17,18	2,9,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,5,12,14,16	2,9,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,5,12	2,9,13	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,5,12,16,17,18	2,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,12,18	2,9,13,15,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,5,12,16,17	2,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,5,12,14,17,18	2,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,5,12,14,16	2,9,13	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,5,12,14,17	2,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,12,14,16,18	2,9,13,15,18	2^{-23}

Table 0.1606 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,5,17,18	2,9,11,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,5,16	2,9,11	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,5,17	2,9,11,15,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,5,16,18	2,9,11,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,5,14	2,9,11	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,5,14,16,17,18	2,9,11,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,5,14,18	2,9,11,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,5,14,16,17	2,9,11,15,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,5,17	2,9,11,13,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,5,16,18	2,9,11,13,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,5,17,18	2,9,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,5,16	2,9,11,13,15	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,14,18	2,9,11,13,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,5,14,16,17	2,9,11,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,14	2,9,11,13,15	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,5,14,16,17,18	2,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,5,12	2,9,11	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,5,12,16,17,18	2,9,11,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,5,12,18	2,9,11,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,5,12,16,17	2,9,11,15,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,5,12,14,17,18	2,9,11,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,5,12,14,16	2,9,11	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,5,12,14,17	2,9,11,15,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,5,12,14,16,18	2,9,11,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,5,12,18	2,9,11,13,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,5,12,16,17	2,9,11,13,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,5,12	2,9,11,13,15	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,5,12,16,17,18	2,9,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,5,12,14,17	2,9,11,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,5,12,14,16,18	2,9,11,13,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,5,12,14,17,18	2,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,5,12,14,16	2,9,11,13,15	2^{-23}

Table 0.1607 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,5,10,18	2,9,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,5,10,16,17	2,9,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,5,10	2,9,15	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,5,10,16,17,18	2,9,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,10,14,17	2,9,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,10,14,16,18	2,9,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,10,14,17,18	2,9,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,10,14,16	2,9,15	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,5,10	2,9,13	2^{-1}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,5,10,16,17,18	2,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,5,10,18	2,9,13,15,18	2^{-1}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,5,10,16,17	2,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,5,10,14,17,18	2,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,5,10,14,16	2,9,13	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,5,10,14,17	2,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,5,10,14,16,18	2,9,13,15,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,5,10,12,17	2,9,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,5,10,12,16,18	2,9,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,5,10,12,17,18	2,9,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,5,10,12,16	2,9,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,5,10,12,14,18	2,9,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,5,10,12,14,16,17	2,9,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,5,10,12,14	2,9,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,5,10,12,14,16,17,18	2,9,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,5,10,12,17,18	2,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,5,10,12,16	2,9,13	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,5,10,12,17	2,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,5,10,12,16,18	2,9,13,15,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,5,10,12,14	2,9,13	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,5,10,12,14,16,17,18	2,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,5,10,12,14,18	2,9,13,15,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,5,10,12,14,16,17	2,9,13,15,17	$2^{-17.5}$

Table 0.1608 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,5,10	2,9,11	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,5,10,16,17,18	2,9,11,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,5,10,18	2,9,11,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,5,10,16,17	2,9,11,15,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,5,10,14,17,18	2,9,11,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,5,10,14,16	2,9,11	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,5,10,14,17	2,9,11,15,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,5,10,14,16,18	2,9,11,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,5,10,18	2,9,11,13,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,5,10,16,17	2,9,11,13,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,5,10	2,9,11,13,15	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,5,10,16,17,18	2,9,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,5,10,14,17	2,9,11,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,5,10,14,16,18	2,9,11,13,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,5,10,14,17,18	2,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,5,10,14,16	2,9,11,13,15	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,5,10,12,17,18	2,9,11,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,5,10,12,16	2,9,11	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,5,10,12,17	2,9,11,15,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,5,10,12,16,18	2,9,11,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,5,10,12,14	2,9,11	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,5,10,12,14,16,17,18	2,9,11,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,5,10,12,14,18	2,9,11,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,5,10,12,14,16,17	2,9,11,15,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,5,10,12,17	2,9,11,13,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,5,10,12,16,18	2,9,11,13,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,5,10,12,17,18	2,9,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,5,10,12,16	2,9,11,13,15	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,5,10,12,14,18	2,9,11,13,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,10,12,14,16,17	2,9,11,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,5,10,12,14	2,9,11,13,15	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,10,12,14,16,17,18	2,9,11,13,15,17,18	$2^{-17.5}$

Table 0.1609 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,5	2,8	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,5,16,17,18	2,8,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,5,18	2,8,15,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,16,17	2,8,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,14,17,18	2,8,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,5,14,16	2,8	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,14,17	2,8,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,14,16,18	2,8,15,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,5,18	2,8,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,5,16,17	2,8,13,17	2^{-1}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,5	2,8,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,5,16,17,18	2,8,13,15,17,18	2^{-1}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,5,14,17	2,8,13,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,5,14,16,18	2,8,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,5,14,17,18	2,8,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,5,14,16	2,8,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,5,12,17,18	2,8,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,5,12,16	2,8	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,5,12,17	2,8,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,5,12,16,18	2,8,15,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,5,12,14	2,8	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,5,12,14,16,17,18	2,8,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,5,12,14,18	2,8,15,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,5,12,14,16,17	2,8,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,5,12,17	2,8,13,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,5,12,16,18	2,8,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,5,12,17,18	2,8,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,5,12,16	2,8,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,5,12,14,18	2,8,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,5,12,14,16,17	2,8,13,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,5,12,14	2,8,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,5,12,14,16,17,18	2,8,13,15,17,18	2^{-12}

Table 0.1610 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,5,18	2,8,11,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,5,16,17	2,8,11,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,5	2,8,11,15	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,5,16,17,18	2,8,11,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,5,14,17	2,8,11,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,5,14,16,18	2,8,11,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,5,14,17,18	2,8,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,5,14,16	2,8,11,15	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,5	2,8,11,13	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,5,16,17,18	2,8,11,13,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,5,18	2,8,11,13,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,5,16,17	2,8,11,13,15,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,5,14,17,18	2,8,11,13,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,5,14,16	2,8,11,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,5,14,17	2,8,11,13,15,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,5,14,16,18	2,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,5,12,17	2,8,11,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,5,12,16,18	2,8,11,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,5,12,17,18	2,8,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,5,12,16	2,8,11,15	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,5,12,14,18	2,8,11,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,5,12,14,16,17	2,8,11,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,5,12,14	2,8,11,15	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,5,12,14,16,17,18	2,8,11,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,5,12,17,18	2,8,11,13,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,5,12,16	2,8,11,13	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,5,12,17	2,8,11,13,15,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,5,12,16,18	2,8,11,13,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,12,14	2,8,11,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,5,12,14,16,17,18	2,8,11,13,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,12,14,18	2,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,5,12,14,16,17	2,8,11,13,15,17	2^{-12}

Table 0.1611 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,5,10,17,18	2,8,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,10,16	2,8	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,5,10,17	2,8,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,10,16,18	2,8,15,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,5,10,14	2,8	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,5,10,14,16,17,18	2,8,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,5,10,14,18	2,8,15,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,5,10,14,16,17	2,8,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,5,10,17	2,8,13,17	2^{-34}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,5,10,16,18	2,8,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,5,10,17,18	2,8,13,15,17,18	2^{-34}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,5,10,16	2,8,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,5,10,14,18	2,8,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,5,10,14,16,17	2,8,13,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,5,10,14	2,8,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,5,10,14,16,17,18	2,8,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,5,10,12	2,8	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,5,10,12,16,17,18	2,8,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,5,10,12,18	2,8,15,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,5,10,12,16,17	2,8,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,5,10,12,14,17,18	2,8,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,5,10,12,14,16	2,8	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,5,10,12,14,17	2,8,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,5,10,12,14,16,18	2,8,15,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,5,10,12,18	2,8,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,5,10,12,16,17	2,8,13,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,5,10,12	2,8,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,5,10,12,16,17,18	2,8,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,10,12,14,17	2,8,13,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,5,10,12,14,16,18	2,8,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,10,12,14,17,18	2,8,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,5,10,12,14,16	2,8,13,15	$2^{-17.5}$

Table 0.1612 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,5,10,17	2,8,11,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,5,10,16,18	2,8,11,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,5,10,17,18	2,8,11,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,5,10,16	2,8,11,15	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,5,10,14,18	2,8,11,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,5,10,14,16,17	2,8,11,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,5,10,14	2,8,11,15	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,5,10,14,16,17,18	2,8,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,5,10,17,18	2,8,11,13,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,5,10,16	2,8,11,13	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,5,10,17	2,8,11,13,15,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,5,10,16,18	2,8,11,13,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,5,10,14	2,8,11,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,10,14,16,17,18	2,8,11,13,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,5,10,14,18	2,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,10,14,16,17	2,8,11,13,15,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,5,10,12,18	2,8,11,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,5,10,12,16,17	2,8,11,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,5,10,12	2,8,11,15	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,5,10,12,16,17,18	2,8,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,5,10,12,14,17	2,8,11,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,5,10,12,14,16,18	2,8,11,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,5,10,12,14,17,18	2,8,11,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,5,10,12,14,16	2,8,11,15	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,5,10,12	2,8,11,13	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,5,10,12,16,17,18	2,8,11,13,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,5,10,12,18	2,8,11,13,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,5,10,12,16,17	2,8,11,13,15,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,5,10,12,14,17,18	2,8,11,13,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,5,10,12,14,16	2,8,11,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,5,10,12,14,17	2,8,11,13,15,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,5,10,12,14,16,18	2,8,11,13,15,18	$2^{-17.5}$

Table 0.1613 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,5,18	2,8,9,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,5,16,17	2,8,9,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,5	2,8,9,15	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,5,16,17,18	2,8,9,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,5,14,17	2,8,9,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,5,14,16,18	2,8,9,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,5,14,17,18	2,8,9,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,5,14,16	2,8,9,15	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,5	2,8,9,13	2^{-34}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,5,16,17,18	2,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,5,18	2,8,9,13,15,18	2^{-34}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,5,16,17	2,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,5,14,17,18	2,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,5,14,16	2,8,9,13	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,5,14,17	2,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,5,14,16,18	2,8,9,13,15,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,5,12,17	2,8,9,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,5,12,16,18	2,8,9,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,5,12,17,18	2,8,9,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,5,12,16	2,8,9,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,5,12,14,18	2,8,9,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,5,12,14,16,17	2,8,9,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,12,14	2,8,9,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,5,12,14,16,17,18	2,8,9,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,5,12,17,18	2,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,5,12,16	2,8,9,13	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,5,12,17	2,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,5,12,16,18	2,8,9,13,15,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,5,12,14	2,8,9,13	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,5,12,14,16,17,18	2,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,5,12,14,18	2,8,9,13,15,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,5,12,14,16,17	2,8,9,13,15,17	$2^{-17.5}$

Table 0.1614 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,5	2,8,9,11	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,5,16,17,18	2,8,9,11,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,18	2,8,9,11,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,5,16,17	2,8,9,11,15,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,5,14,17,18	2,8,9,11,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,5,14,16	2,8,9,11	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,5,14,17	2,8,9,11,15,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,5,14,16,18	2,8,9,11,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,5,18	2,8,9,11,13,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,5,16,17	2,8,9,11,13,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,5	2,8,9,11,13,15	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,5,16,17,18	2,8,9,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,5,14,17	2,8,9,11,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,5,14,16,18	2,8,9,11,13,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,5,14,17,18	2,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,5,14,16	2,8,9,11,13,15	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,5,12,17,18	2,8,9,11,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,5,12,16	2,8,9,11	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,5,12,17	2,8,9,11,15,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,5,12,16,18	2,8,9,11,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,5,12,14	2,8,9,11	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,12,14,16,17,18	2,8,9,11,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,5,12,14,18	2,8,9,11,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,5,12,14,16,17	2,8,9,11,15,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,5,12,17	2,8,9,11,13,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,5,12,16,18	2,8,9,11,13,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,5,12,17,18	2,8,9,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,5,12,16	2,8,9,11,13,15	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,5,12,14,18	2,8,9,11,13,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,5,12,14,16,17	2,8,9,11,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,5,12,14	2,8,9,11,13,15	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,5,12,14,16,17,18	2,8,9,11,13,15,17,18	$2^{-17.5}$

Table 0.1615 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,5,10,17	2,8,9,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,5,10,16,18	2,8,9,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,5,10,17,18	2,8,9,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,5,10,16	2,8,9,15	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,10,14,18	2,8,9,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,5,10,14,16,17	2,8,9,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,10,14	2,8,9,15	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,5,10,14,16,17,18	2,8,9,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,5,10,17,18	2,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,5,10,16	2,8,9,13	2^{-1}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,5,10,17	2,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,5,10,16,18	2,8,9,13,15,18	2^{-1}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,5,10,14	2,8,9,13	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,5,10,14,16,17,18	2,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,5,10,14,18	2,8,9,13,15,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,5,10,14,16,17	2,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,5,10,12,18	2,8,9,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,5,10,12,16,17	2,8,9,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,5,10,12	2,8,9,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,5,10,12,16,17,18	2,8,9,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,5,10,12,14,17	2,8,9,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,5,10,12,14,16,18	2,8,9,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,5,10,12,14,17,18	2,8,9,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,5,10,12,14,16	2,8,9,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,5,10,12	2,8,9,13	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,5,10,12,16,17,18	2,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,5,10,12,18	2,8,9,13,15,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,5,10,12,16,17	2,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,5,10,12,14,17,18	2,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,5,10,12,14,16	2,8,9,13	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,5,10,12,14,17	2,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,5,10,12,14,16,18	2,8,9,13,15,18	2^{-12}

Table 0.1616 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,5,10,17,18	2,8,9,11,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,5,10,16	2,8,9,11	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,5,10,17	2,8,9,11,15,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,5,10,16,18	2,8,9,11,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,10,14	2,8,9,11	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,5,10,14,16,17,18	2,8,9,11,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,10,14,18	2,8,9,11,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,5,10,14,16,17	2,8,9,11,15,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,5,10,17	2,8,9,11,13,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,10,16,18	2,8,9,11,13,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,5,10,17,18	2,8,9,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,10,16	2,8,9,11,13,15	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,5,10,14,18	2,8,9,11,13,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,5,10,14,16,17	2,8,9,11,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,5,10,14	2,8,9,11,13,15	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,5,10,14,16,17,18	2,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,5,10,12	2,8,9,11	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,5,10,12,16,17,18	2,8,9,11,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,5,10,12,18	2,8,9,11,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,5,10,12,16,17	2,8,9,11,15,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,5,10,12,14,17,18	2,8,9,11,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,5,10,12,14,16	2,8,9,11	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,5,10,12,14,17	2,8,9,11,15,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,5,10,12,14,16,18	2,8,9,11,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,5,10,12,18	2,8,9,11,13,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,5,10,12,16,17	2,8,9,11,13,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,5,10,12	2,8,9,11,13,15	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,5,10,12,16,17,18	2,8,9,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,5,10,12,14,17	2,8,9,11,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,5,10,12,14,16,18	2,8,9,11,13,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,5,10,12,14,17,18	2,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,5,10,12,14,16	2,8,9,11,13,15	2^{-12}

Table 0.1617 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,5,7,17	2,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,5,7,16,18	2,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,5,7,17,18	2,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,5,7,16	2,15	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,5,7,14,18	2,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,5,7,14,16,17	2,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,5,7,14	2,15	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,5,7,14,16,17,18	2,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,5,7,17,18	2,13,17,18	2^{-1}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,5,7,16	2,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,5,7,17	2,13,15,17	2^{-1}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,5,7,16,18	2,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,7,14	2,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,5,7,14,16,17,18	2,13,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,7,14,18	2,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,5,7,14,16,17	2,13,15,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,5,7,12,18	2,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,5,7,12,16,17	2,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,5,7,12	2,15	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,5,7,12,16,17,18	2,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,5,7,12,14,17	2,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,5,7,12,14,16,18	2,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,5,7,12,14,17,18	2,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,5,7,12,14,16	2,15	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,5,7,12	2,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,5,7,12,16,17,18	2,13,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,5,7,12,18	2,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,5,7,12,16,17	2,13,15,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,5,7,12,14,17,18	2,13,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,5,7,12,14,16	2,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,5,7,12,14,17	2,13,15,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,5,7,12,14,16,18	2,13,15,18	$2^{-17.5}$

Table 0.1618 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,17,18	2,11,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,5,7,16	2,11	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,17	2,11,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,5,7,16,18	2,11,15,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,5,7,14	2,11	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,5,7,14,16,17,18	2,11,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,5,7,14,18	2,11,15,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,5,7,14,16,17	2,11,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,5,7,17	2,11,13,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,5,7,16,18	2,11,13,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,5,7,17,18	2,11,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,5,7,16	2,11,13,15	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,5,7,14,18	2,11,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,5,7,14,16,17	2,11,13,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,5,7,14	2,11,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,5,7,14,16,17,18	2,11,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,5,7,12	2,11	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,5,7,12,16,17,18	2,11,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,5,7,12,18	2,11,15,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,5,7,12,16,17	2,11,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,12,14,17,18	2,11,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,12,14,16	2,11	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,12,14,17	2,11,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,12,14,16,18	2,11,15,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,5,7,12,18	2,11,13,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,5,7,12,16,17	2,11,13,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,5,7,12	2,11,13,15	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,5,7,12,16,17,18	2,11,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,5,7,12,14,17	2,11,13,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,7,12,14,16,18	2,11,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,5,7,12,14,17,18	2,11,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,7,12,14,16	2,11,13,15	$2^{-17.5}$

Table 0.1619 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,5,7,10,18	2,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,5,7,10,16,17	2,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,5,7,10	2,15	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,5,7,10,16,17,18	2,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,5,7,10,14,17	2,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,5,7,10,14,16,18	2,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,5,7,10,14,17,18	2,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,5,7,10,14,16	2,15	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,5,7,10	2,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,5,7,10,16,17,18	2,13,17,18	2^{-34}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,5,7,10,18	2,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,5,7,10,16,17	2,13,15,17	2^{-34}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,5,7,10,14,17,18	2,13,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,5,7,10,14,16	2,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,5,7,10,14,17	2,13,15,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,5,7,10,14,16,18	2,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,5,7,10,12,17	2,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,5,7,10,12,16,18	2,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,5,7,10,12,17,18	2,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,5,7,10,12,16	2,15	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,5,7,10,12,14,18	2,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,5,7,10,12,14,16,17	2,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,5,7,10,12,14	2,15	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,5,7,10,12,14,16,17,18	2,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,5,7,10,12,17,18	2,13,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,5,7,10,12,16	2,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,5,7,10,12,17	2,13,15,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,5,7,10,12,16,18	2,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,5,7,10,12,14	2,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,7,10,12,14,16,17,18	2,13,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,5,7,10,12,14,18	2,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,7,10,12,14,16,17	2,13,15,17	2^{-23}

Table 0.1620 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,10	2,11	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,5,7,10,16,17,18	2,11,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,10,18	2,11,15,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,5,7,10,16,17	2,11,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,10,14,17,18	2,11,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,10,14,16	2,11	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,10,14,17	2,11,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,10,14,16,18	2,11,15,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,5,7,10,18	2,11,13,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,5,7,10,16,17	2,11,13,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,5,7,10	2,11,13,15	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,5,7,10,16,17,18	2,11,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,10,14,17	2,11,13,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,5,7,10,14,16,18	2,11,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,10,14,17,18	2,11,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,5,7,10,14,16	2,11,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,5,7,10,12,17,18	2,11,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,5,7,10,12,16	2,11	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,5,7,10,12,17	2,11,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,5,7,10,12,16,18	2,11,15,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,5,7,10,12,14	2,11	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5,7,10,12,14,16,17,18	2,11,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,5,7,10,12,14,18	2,11,15,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,5,7,10,12,14,16,17	2,11,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,5,7,10,12,17	2,11,13,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,7,10,12,16,18	2,11,13,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,5,7,10,12,17,18	2,11,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,5,7,10,12,16	2,11,13,15	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,5,7,10,12,14,18	2,11,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,5,7,10,12,14,16,17	2,11,13,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,5,7,10,12,14	2,11,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,5,7,10,12,14,16,17,18	2,11,13,15,17,18	2^{-23}

Table 0.1621 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,5,7,17,18	2,9,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,5,7,16	2,9	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,5,7,17	2,9,15,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,5,7,16,18	2,9,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,5,7,14	2,9	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,7,14,16,17,18	2,9,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,5,7,14,18	2,9,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,7,14,16,17	2,9,15,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,5,7,17	2,9,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,5,7,16,18	2,9,13,18	2^{-34}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,5,7,17,18	2,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,5,7,16	2,9,13,15	2^{-34}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,5,7,14,18	2,9,13,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,5,7,14,16,17	2,9,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,5,7,14	2,9,13,15	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,5,7,14,16,17,18	2,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,5,7,12	2,9	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,5,7,12,16,17,18	2,9,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,5,7,12,18	2,9,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,5,7,12,16,17	2,9,15,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,12,14,17,18	2,9,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,5,7,12,14,16	2,9	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,12,14,17	2,9,15,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,5,7,12,14,16,18	2,9,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5,7,12,18	2,9,13,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,5,7,12,16,17	2,9,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5,7,12	2,9,13,15	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,5,7,12,16,17,18	2,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,12,14,17	2,9,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,5,7,12,14,16,18	2,9,13,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,5,7,12,14,17,18	2,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,5,7,12,14,16	2,9,13,15	2^{-23}

Table 0.1622 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,5,7,17	2,9,11,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,5,7,16,18	2,9,11,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,5,7,17,18	2,9,11,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,5,7,16	2,9,11,15	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,5,7,14,18	2,9,11,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,7,14,16,17	2,9,11,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,5,7,14	2,9,11,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,7,14,16,17,18	2,9,11,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,5,7,17,18	2,9,11,13,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,5,7,16	2,9,11,13	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,5,7,17	2,9,11,13,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,5,7,16,18	2,9,11,13,15,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,5,7,14	2,9,11,13	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,5,7,14,16,17,18	2,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,5,7,14,18	2,9,11,13,15,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,5,7,14,16,17	2,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,5,7,12,18	2,9,11,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,5,7,12,16,17	2,9,11,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,5,7,12	2,9,11,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,5,7,12,16,17,18	2,9,11,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,5,7,12,14,17	2,9,11,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,7,12,14,16,18	2,9,11,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,5,7,12,14,17,18	2,9,11,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,5,7,12,14,16	2,9,11,15	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,5,7,12	2,9,11,13	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,5,7,12,16,17,18	2,9,11,13,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,5,7,12,18	2,9,11,13,15,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,5,7,12,16,17	2,9,11,13,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,5,7,12,14,17,18	2,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,5,7,12,14,16	2,9,11,13	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,5,7,12,14,17	2,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,5,7,12,14,16,18	2,9,11,13,15,18	2^{-23}

Table 0.1623 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,5,7,10	2,9	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,5,7,10,16,17,18	2,9,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,5,7,10,18	2,9,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,5,7,10,16,17	2,9,15,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,5,7,10,14,17,18	2,9,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,5,7,10,14,16	2,9	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,5,7,10,14,17	2,9,15,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,5,7,10,14,16,18	2,9,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,5,7,10,18	2,9,13,18	2^{-1}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,5,7,10,16,17	2,9,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,5,7,10	2,9,13,15	2^{-1}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,5,7,10,16,17,18	2,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,5,7,10,14,17	2,9,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,5,7,10,14,16,18	2,9,13,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,5,7,10,14,17,18	2,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,5,7,10,14,16	2,9,13,15	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,5,7,10,12,17,18	2,9,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,5,7,10,12,16	2,9	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,5,7,10,12,17	2,9,15,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,5,7,10,12,16,18	2,9,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,5,7,10,12,14	2,9	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,5,7,10,12,14,16,17,18	2,9,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,5,7,10,12,14,18	2,9,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,5,7,10,12,14,16,17	2,9,15,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,5,7,10,12,17	2,9,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,5,7,10,12,16,18	2,9,13,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,5,7,10,12,17,18	2,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,5,7,10,12,16	2,9,13,15	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,5,7,10,12,14,18	2,9,13,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,5,7,10,12,14,16,17	2,9,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,5,7,10,12,14	2,9,13,15	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,5,7,10,12,14,16,17,18	2,9,13,15,17,18	$2^{-17.5}$

Table 0.1624 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,5,7,10,18	2,9,11,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,5,7,10,16,17	2,9,11,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,5,7,10	2,9,11,15	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,5,7,10,16,17,18	2,9,11,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,5,7,10,14,17	2,9,11,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,5,7,10,14,16,18	2,9,11,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,5,7,10,14,17,18	2,9,11,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,5,7,10,14,16	2,9,11,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,5,7,10	2,9,11,13	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,5,7,10,16,17,18	2,9,11,13,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,5,7,10,18	2,9,11,13,15,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,5,7,10,16,17	2,9,11,13,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,5,7,10,14,17,18	2,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,5,7,10,14,16	2,9,11,13	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,5,7,10,14,17	2,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,5,7,10,14,16,18	2,9,11,13,15,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,5,7,10,12,17	2,9,11,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,5,7,10,12,16,18	2,9,11,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,10,12,17,18	2,9,11,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,5,7,10,12,16	2,9,11,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,5,7,10,12,14,18	2,9,11,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,5,7,10,12,14,16,17	2,9,11,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,5,7,10,12,14	2,9,11,15	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,5,7,10,12,14,16,17,18	2,9,11,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,5,7,10,12,17,18	2,9,11,13,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,5,7,10,12,16	2,9,11,13	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,5,7,10,12,17	2,9,11,13,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,5,7,10,12,16,18	2,9,11,13,15,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,5,7,10,12,14	2,9,11,13	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,5,7,10,12,14,16,17,18	2,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,5,7,10,12,14,18	2,9,11,13,15,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,5,7,10,12,14,16,17	2,9,11,13,15,17	$2^{-17.5}$

Table 0.1625 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,5,7,18	2,8,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,5,7,16,17	2,8,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,5,7	2,8,15	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,5,7,16,17,18	2,8,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,5,7,14,17	2,8,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,5,7,14,16,18	2,8,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,5,7,14,17,18	2,8,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,5,7,14,16	2,8,15	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,5,7	2,8,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,5,7,16,17,18	2,8,13,17,18	2^{-1}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,5,7,18	2,8,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,5,7,16,17	2,8,13,15,17	2^{-1}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,5,7,14,17,18	2,8,13,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,5,7,14,16	2,8,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,5,7,14,17	2,8,13,15,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,5,7,14,16,18	2,8,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,5,7,12,17	2,8,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,5,7,12,16,18	2,8,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,5,7,12,17,18	2,8,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,5,7,12,16	2,8,15	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,5,7,12,14,18	2,8,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,7,12,14,16,17	2,8,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,5,7,12,14	2,8,15	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,5,7,12,14,16,17,18	2,8,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,5,7,12,17,18	2,8,13,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,5,7,12,16	2,8,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,5,7,12,17	2,8,13,15,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,5,7,12,16,18	2,8,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,5,7,12,14	2,8,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,5,7,12,14,16,17,18	2,8,13,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,5,7,12,14,18	2,8,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,5,7,12,14,16,17	2,8,13,15,17	2^{-12}

Table 0.1626 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,5,7	2,8,11	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,5,7,16,17,18	2,8,11,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,5,7,18	2,8,11,15,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,5,7,16,17	2,8,11,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,5,7,14,17,18	2,8,11,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,5,7,14,16	2,8,11	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,5,7,14,17	2,8,11,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,5,7,14,16,18	2,8,11,15,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,5,7,18	2,8,11,13,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,5,7,16,17	2,8,11,13,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,5,7	2,8,11,13,15	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,5,7,16,17,18	2,8,11,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,5,7,14,17	2,8,11,13,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,5,7,14,16,18	2,8,11,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,5,7,14,17,18	2,8,11,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,5,7,14,16	2,8,11,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,5,7,12,17,18	2,8,11,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,12,16	2,8,11	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,5,7,12,17	2,8,11,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,12,16,18	2,8,11,15,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,5,7,12,14	2,8,11	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,5,7,12,14,16,17,18	2,8,11,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,5,7,12,14,18	2,8,11,15,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,5,7,12,14,16,17	2,8,11,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,5,7,12,17	2,8,11,13,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,5,7,12,16,18	2,8,11,13,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,5,7,12,17,18	2,8,11,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,5,7,12,16	2,8,11,13,15	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,5,7,12,14,18	2,8,11,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,5,7,12,14,16,17	2,8,11,13,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,5,7,12,14	2,8,11,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,5,7,12,14,16,17,18	2,8,11,13,15,17,18	2^{-12}

Table 0.1627 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,5,7,10,17	2,8,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,5,7,10,16,18	2,8,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,5,7,10,17,18	2,8,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,5,7,10,16	2,8,15	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,7,10,14,18	2,8,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,5,7,10,14,16,17	2,8,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,7,10,14	2,8,15	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,5,7,10,14,16,17,18	2,8,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,5,7,10,17,18	2,8,13,17,18	2^{-34}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,10,16	2,8,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,5,7,10,17	2,8,13,15,17	2^{-34}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,10,16,18	2,8,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,5,7,10,14	2,8,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,5,7,10,14,16,17,18	2,8,13,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,5,7,10,14,18	2,8,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,5,7,10,14,16,17	2,8,13,15,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,5,7,10,12,18	2,8,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,5,7,10,12,16,17	2,8,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,5,7,10,12	2,8,15	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,5,7,10,12,16,17,18	2,8,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,5,7,10,12,14,17	2,8,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,5,7,10,12,14,16,18	2,8,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,5,7,10,12,14,17,18	2,8,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,5,7,10,12,14,16	2,8,15	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,5,7,10,12	2,8,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,5,7,10,12,16,17,18	2,8,13,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,5,7,10,12,18	2,8,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,5,7,10,12,16,17	2,8,13,15,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,5,7,10,12,14,17,18	2,8,13,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,5,7,10,12,14,16	2,8,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,5,7,10,12,14,17	2,8,13,15,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,5,7,10,12,14,16,18	2,8,13,15,18	$2^{-17.5}$

Table 0.1628 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,5,7,10,17,18	2,8,11,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,5,7,10,16	2,8,11	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,5,7,10,17	2,8,11,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,5,7,10,16,18	2,8,11,15,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,7,10,14	2,8,11	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,5,7,10,14,16,17,18	2,8,11,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,7,10,14,18	2,8,11,15,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,5,7,10,14,16,17	2,8,11,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,5,7,10,17	2,8,11,13,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,5,7,10,16,18	2,8,11,13,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,5,7,10,17,18	2,8,11,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,5,7,10,16	2,8,11,13,15	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,5,7,10,14,18	2,8,11,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,5,7,10,14,16,17	2,8,11,13,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,5,7,10,14	2,8,11,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,5,7,10,14,16,17,18	2,8,11,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,5,7,10,12	2,8,11	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,5,7,10,12,16,17,18	2,8,11,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,5,7,10,12,18	2,8,11,15,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,7,10,12,16,17	2,8,11,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,5,7,10,12,14,17,18	2,8,11,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,5,7,10,12,14,16	2,8,11	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,5,7,10,12,14,17	2,8,11,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,5,7,10,12,14,16,18	2,8,11,15,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,5,7,10,12,18	2,8,11,13,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,5,7,10,12,16,17	2,8,11,13,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,5,7,10,12	2,8,11,13,15	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,5,7,10,12,16,17,18	2,8,11,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,5,7,10,12,14,17	2,8,11,13,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,5,7,10,12,14,16,18	2,8,11,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,5,7,10,12,14,17,18	2,8,11,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,5,7,10,12,14,16	2,8,11,13,15	$2^{-17.5}$

Table 0.1629 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,5,7	2,8,9	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,5,7,16,17,18	2,8,9,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,5,7,18	2,8,9,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,5,7,16,17	2,8,9,15,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,5,7,14,17,18	2,8,9,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,5,7,14,16	2,8,9	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,5,7,14,17	2,8,9,15,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,5,7,14,16,18	2,8,9,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,5,7,18	2,8,9,13,18	2^{-34}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,5,7,16,17	2,8,9,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,5,7	2,8,9,13,15	2^{-34}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,5,7,16,17,18	2,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,5,7,14,17	2,8,9,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,5,7,14,16,18	2,8,9,13,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,5,7,14,17,18	2,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,5,7,14,16	2,8,9,13,15	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,5,7,12,17,18	2,8,9,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,5,7,12,16	2,8,9	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,5,7,12,17	2,8,9,15,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,5,7,12,16,18	2,8,9,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,5,7,12,14	2,8,9	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,5,7,12,14,16,17,18	2,8,9,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,5,7,12,14,18	2,8,9,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,5,7,12,14,16,17	2,8,9,15,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,5,7,12,17	2,8,9,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,5,7,12,16,18	2,8,9,13,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,5,7,12,17,18	2,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,5,7,12,16	2,8,9,13,15	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,7,12,14,18	2,8,9,13,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,5,7,12,14,16,17	2,8,9,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,7,12,14	2,8,9,13,15	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,5,7,12,14,16,17,18	2,8,9,13,15,17,18	$2^{-17.5}$

Table 0.1630 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,5,7,18	2,8,9,11,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,16,17	2,8,9,11,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,5,7	2,8,9,11,15	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,16,17,18	2,8,9,11,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,14,17	2,8,9,11,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,14,16,18	2,8,9,11,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,14,17,18	2,8,9,11,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,14,16	2,8,9,11,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,5,7	2,8,9,11,13	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,5,7,16,17,18	2,8,9,11,13,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,5,7,18	2,8,9,11,13,15,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,5,7,16,17	2,8,9,11,13,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,5,7,14,17,18	2,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,14,16	2,8,9,11,13	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,5,7,14,17	2,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,14,16,18	2,8,9,11,13,15,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,5,7,12,17	2,8,9,11,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,5,7,12,16,18	2,8,9,11,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,5,7,12,17,18	2,8,9,11,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,5,7,12,16	2,8,9,11,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,5,7,12,14,18	2,8,9,11,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,5,7,12,14,16,17	2,8,9,11,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,5,7,12,14	2,8,9,11,15	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,5,7,12,14,16,17,18	2,8,9,11,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,5,7,12,17,18	2,8,9,11,13,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,5,7,12,16	2,8,9,11,13	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,5,7,12,17	2,8,9,11,13,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,5,7,12,16,18	2,8,9,11,13,15,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,5,7,12,14	2,8,9,11,13	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,5,7,12,14,16,17,18	2,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,5,7,12,14,18	2,8,9,11,13,15,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,5,7,12,14,16,17	2,8,9,11,13,15,17	$2^{-17.5}$

Table 0.1631 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,5,7,10,17,18	2,8,9,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,5,7,10,16	2,8,9	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,5,7,10,17	2,8,9,15,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,5,7,10,16,18	2,8,9,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,5,7,10,14	2,8,9	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,5,7,10,14,16,17,18	2,8,9,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,5,7,10,14,18	2,8,9,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,5,7,10,14,16,17	2,8,9,15,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,5,7,10,17	2,8,9,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,5,7,10,16,18	2,8,9,13,18	2^{-1}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,5,7,10,17,18	2,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,5,7,10,16	2,8,9,13,15	2^{-1}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,5,7,10,14,18	2,8,9,13,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,7,10,14,16,17	2,8,9,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,5,7,10,14	2,8,9,13,15	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,7,10,14,16,17,18	2,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,5,7,10,12	2,8,9	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,5,7,10,12,16,17,18	2,8,9,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,5,7,10,12,18	2,8,9,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,5,7,10,12,16,17	2,8,9,15,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,5,7,10,12,14,17,18	2,8,9,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,5,7,10,12,14,16	2,8,9	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,5,7,10,12,14,17	2,8,9,15,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,5,7,10,12,14,16,18	2,8,9,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,5,7,10,12,18	2,8,9,13,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,5,7,10,12,16,17	2,8,9,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,5,7,10,12	2,8,9,13,15	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,5,7,10,12,16,17,18	2,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,5,7,10,12,14,17	2,8,9,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,5,7,10,12,14,16,18	2,8,9,13,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,5,7,10,12,14,17,18	2,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,5,7,10,12,14,16	2,8,9,13,15	2^{-12}

Table 0.1632 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,5,7,10,17	2,8,9,11,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,10,16,18	2,8,9,11,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,5,7,10,17,18	2,8,9,11,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,10,16	2,8,9,11,15	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,5,7,10,14,18	2,8,9,11,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,5,7,10,14,16,17	2,8,9,11,17	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,5,7,10,14	2,8,9,11,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,5,7,10,14,16,17,18	2,8,9,11,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,5,7,10,17,18	2,8,9,11,13,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,5,7,10,16	2,8,9,11,13	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,5,7,10,17	2,8,9,11,13,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,5,7,10,16,18	2,8,9,11,13,15,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,5,7,10,14	2,8,9,11,13	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,5,7,10,14,16,17,18	2,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,5,7,10,14,18	2,8,9,11,13,15,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,5,7,10,14,16,17	2,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,5,7,10,12,18	2,8,9,11,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,5,7,10,12,16,17	2,8,9,11,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,5,7,10,12	2,8,9,11,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,5,7,10,12,16,17,18	2,8,9,11,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,10,12,14,17	2,8,9,11,17	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,10,12,14,16,18	2,8,9,11,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,10,12,14,17,18	2,8,9,11,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,10,12,14,16	2,8,9,11,15	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,5,7,10,12	2,8,9,11,13	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,5,7,10,12,16,17,18	2,8,9,11,13,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,5,7,10,12,18	2,8,9,11,13,15,18	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,5,7,10,12,16,17	2,8,9,11,13,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,7,10,12,14,17,18	2,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,5,7,10,12,14,16	2,8,9,11,13	2^{-12}
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,7,10,12,14,17	2,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,5,7,10,12,14,16,18	2,8,9,11,13,15,18	2^{-12}

Table 0.1633 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,5	2,6	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,5,16,17,18	2,6,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,5,18	2,6,15,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,5,16,17	2,6,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,5,14,17,18	2,6,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,5,14,16	2,6	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,5,14,17	2,6,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,5,14,16,18	2,6,15,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,5,18	2,6,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,5,16,17	2,6,13,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,5	2,6,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,5,16,17,18	2,6,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,5,14,17	2,6,13,17	2^{-1}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,5,14,16,18	2,6,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,5,14,17,18	2,6,13,15,17,18	2^{-1}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,5,14,16	2,6,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,5,12,17,18	2,6,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,5,12,16	2,6	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,5,12,17	2,6,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,5,12,16,18	2,6,15,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,5,12,14	2,6	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,5,12,14,16,17,18	2,6,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,5,12,14,18	2,6,15,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,5,12,14,16,17	2,6,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,5,12,17	2,6,13,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,5,12,16,18	2,6,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,5,12,17,18	2,6,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,5,12,16	2,6,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,5,12,14,18	2,6,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,5,12,14,16,17	2,6,13,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,5,12,14	2,6,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,5,12,14,16,17,18	2,6,13,15,17,18	2^{-23}

Table 0.1634 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,18	2,6,11,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,5,16,17	2,6,11,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5	2,6,11,15	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,5,16,17,18	2,6,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,5,14,17	2,6,11,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,5,14,16,18	2,6,11,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,5,14,17,18	2,6,11,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,5,14,16	2,6,11,15	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5	2,6,11,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,5,16,17,18	2,6,11,13,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,5,18	2,6,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,5,16,17	2,6,11,13,15,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,5,14,17,18	2,6,11,13,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,5,14,16	2,6,11,13	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,5,14,17	2,6,11,13,15,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,5,14,16,18	2,6,11,13,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,5,12,17	2,6,11,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,5,12,16,18	2,6,11,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,5,12,17,18	2,6,11,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,5,12,16	2,6,11,15	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,5,12,14,18	2,6,11,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,5,12,14,16,17	2,6,11,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,5,12,14	2,6,11,15	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,5,12,14,16,17,18	2,6,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,5,12,17,18	2,6,11,13,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,5,12,16	2,6,11,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,5,12,17	2,6,11,13,15,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,5,12,16,18	2,6,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,5,12,14	2,6,11,13	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,5,12,14,16,17,18	2,6,11,13,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,5,12,14,18	2,6,11,13,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,5,12,14,16,17	2,6,11,13,15,17	2^{-12}

Table 0.1635 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,5,10,17,18	2,6,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,5,10,16	2,6	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,5,10,17	2,6,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,5,10,16,18	2,6,15,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,5,10,14	2,6	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,5,10,14,16,17,18	2,6,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,5,10,14,18	2,6,15,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,5,10,14,16,17	2,6,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,5,10,17	2,6,13,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,5,10,16,18	2,6,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,5,10,17,18	2,6,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,5,10,16	2,6,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,5,10,14,18	2,6,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,5,10,14,16,17	2,6,13,17	2^{-34}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,5,10,14	2,6,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,5,10,14,16,17,18	2,6,13,15,17,18	2^{-34}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,5,10,12	2,6	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,10,12,16,17,18	2,6,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,5,10,12,18	2,6,15,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,10,12,16,17	2,6,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,5,10,12,14,17,18	2,6,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,5,10,12,14,16	2,6	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,5,10,12,14,17	2,6,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,5,10,12,14,16,18	2,6,15,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,5,10,12,18	2,6,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,5,10,12,16,17	2,6,13,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,5,10,12	2,6,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,5,10,12,16,17,18	2,6,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,5,10,12,14,17	2,6,13,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,5,10,12,14,16,18	2,6,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,5,10,12,14,17,18	2,6,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,5,10,12,14,16	2,6,13,15	$2^{-17.5}$

Table 0.1636 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,5,10,17	2,6,11,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,5,10,16,18	2,6,11,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,5,10,17,18	2,6,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,5,10,16	2,6,11,15	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,5,10,14,18	2,6,11,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,5,10,14,16,17	2,6,11,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,5,10,14	2,6,11,15	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,5,10,14,16,17,18	2,6,11,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,5,10,17,18	2,6,11,13,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,5,10,16	2,6,11,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,5,10,17	2,6,11,13,15,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,5,10,16,18	2,6,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,5,10,14	2,6,11,13	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,5,10,14,16,17,18	2,6,11,13,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,5,10,14,18	2,6,11,13,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,5,10,14,16,17	2,6,11,13,15,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,5,10,12,18	2,6,11,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,10,12,16,17	2,6,11,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,5,10,12	2,6,11,15	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,10,12,16,17,18	2,6,11,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,5,10,12,14,17	2,6,11,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,5,10,12,14,16,18	2,6,11,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,5,10,12,14,17,18	2,6,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,5,10,12,14,16	2,6,11,15	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,5,10,12	2,6,11,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,5,10,12,16,17,18	2,6,11,13,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,5,10,12,18	2,6,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,5,10,12,16,17	2,6,11,13,15,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,10,12,14,17,18	2,6,11,13,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,5,10,12,14,16	2,6,11,13	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,10,12,14,17	2,6,11,13,15,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,5,10,12,14,16,18	2,6,11,13,15,18	$2^{-28.5}$

Table 0.1637 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,5,18	2,6,9,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,5,16,17	2,6,9,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,5	2,6,9,15	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,5,16,17,18	2,6,9,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,5,14,17	2,6,9,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,5,14,16,18	2,6,9,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,5,14,17,18	2,6,9,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,5,14,16	2,6,9,15	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,5	2,6,9,13	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,5,16,17,18	2,6,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,5,18	2,6,9,13,15,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,5,16,17	2,6,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,5,14,17,18	2,6,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,5,14,16	2,6,9,13	2^{-34}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,5,14,17	2,6,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,5,14,16,18	2,6,9,13,15,18	2^{-34}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,12,17	2,6,9,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,12,16,18	2,6,9,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,12,17,18	2,6,9,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,12,16	2,6,9,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,5,12,14,18	2,6,9,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,5,12,14,16,17	2,6,9,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,5,12,14	2,6,9,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,5,12,14,16,17,18	2,6,9,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,5,12,17,18	2,6,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,5,12,16	2,6,9,13	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,5,12,17	2,6,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,5,12,16,18	2,6,9,13,15,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,5,12,14	2,6,9,13	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,5,12,14,16,17,18	2,6,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,5,12,14,18	2,6,9,13,15,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,5,12,14,16,17	2,6,9,13,15,17	$2^{-17.5}$

Table 0.1638 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,5	2,6,9,11	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,5,16,17,18	2,6,9,11,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,5,18	2,6,9,11,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,5,16,17	2,6,9,11,15,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,5,14,17,18	2,6,9,11,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,5,14,16	2,6,9,11	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,5,14,17	2,6,9,11,15,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,5,14,16,18	2,6,9,11,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,5,18	2,6,9,11,13,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,16,17	2,6,9,11,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,5	2,6,9,11,13,15	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,16,17,18	2,6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,5,14,17	2,6,9,11,13,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,5,14,16,18	2,6,9,11,13,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,5,14,17,18	2,6,9,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,5,14,16	2,6,9,11,13,15	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,5,12,17,18	2,6,9,11,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,5,12,16	2,6,9,11	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,5,12,17	2,6,9,11,15,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,5,12,16,18	2,6,9,11,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,5,12,14	2,6,9,11	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,5,12,14,16,17,18	2,6,9,11,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,5,12,14,18	2,6,9,11,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,5,12,14,16,17	2,6,9,11,15,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,5,12,17	2,6,9,11,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,5,12,16,18	2,6,9,11,13,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,5,12,17,18	2,6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,5,12,16	2,6,9,11,13,15	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,5,12,14,18	2,6,9,11,13,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,5,12,14,16,17	2,6,9,11,13,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,5,12,14	2,6,9,11,13,15	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,5,12,14,16,17,18	2,6,9,11,13,15,17,18	$2^{-28.5}$

Table 0.1639 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,5,10,17	2,6,9,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,5,10,16,18	2,6,9,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,5,10,17,18	2,6,9,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,5,10,16	2,6,9,15	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,5,10,14,18	2,6,9,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,5,10,14,16,17	2,6,9,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,5,10,14	2,6,9,15	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,5,10,14,16,17,18	2,6,9,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,5,10,17,18	2,6,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,10,16	2,6,9,13	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,5,10,17	2,6,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,10,16,18	2,6,9,13,15,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,5,10,14	2,6,9,13	2^{-1}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,5,10,14,16,17,18	2,6,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,5,10,14,18	2,6,9,13,15,18	2^{-1}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,5,10,14,16,17	2,6,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,5,10,12,18	2,6,9,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,5,10,12,16,17	2,6,9,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,5,10,12	2,6,9,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,5,10,12,16,17,18	2,6,9,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,5,10,12,14,17	2,6,9,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,5,10,12,14,16,18	2,6,9,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,5,10,12,14,17,18	2,6,9,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,5,10,12,14,16	2,6,9,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,5,10,12	2,6,9,13	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,5,10,12,16,17,18	2,6,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,5,10,12,18	2,6,9,13,15,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,10,12,16,17	2,6,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,5,10,12,14,17,18	2,6,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,5,10,12,14,16	2,6,9,13	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,10,12,14,17	2,6,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,5,10,12,14,16,18	2,6,9,13,15,18	2^{-23}

Table 0.1640 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,5,10,17,18	2,6,9,11,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,5,10,16	2,6,9,11	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,5,10,17	2,6,9,11,15,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,5,10,16,18	2,6,9,11,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,5,10,14	2,6,9,11	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,5,10,14,16,17,18	2,6,9,11,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,5,10,14,18	2,6,9,11,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,5,10,14,16,17	2,6,9,11,15,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,5,10,17	2,6,9,11,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,5,10,16,18	2,6,9,11,13,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,10,17,18	2,6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,5,10,16	2,6,9,11,13,15	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,5,10,14,18	2,6,9,11,13,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,5,10,14,16,17	2,6,9,11,13,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,5,10,14	2,6,9,11,13,15	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,5,10,14,16,17,18	2,6,9,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,5,10,12	2,6,9,11	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,5,10,12,16,17,18	2,6,9,11,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,5,10,12,18	2,6,9,11,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,5,10,12,16,17	2,6,9,11,15,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,5,10,12,14,17,18	2,6,9,11,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,5,10,12,14,16	2,6,9,11	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,5,10,12,14,17	2,6,9,11,15,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,5,10,12,14,16,18	2,6,9,11,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,10,12,18	2,6,9,11,13,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,5,10,12,16,17	2,6,9,11,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,10,12	2,6,9,11,13,15	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,5,10,12,16,17,18	2,6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,5,10,12,14,17	2,6,9,11,13,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,5,10,12,14,16,18	2,6,9,11,13,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,5,10,12,14,17,18	2,6,9,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,5,10,12,14,16	2,6,9,11,13,15	2^{-12}

Table 0.1641 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,5,17,18	2,6,8,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,5,16	2,6,8	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,5,17	2,6,8,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,5,16,18	2,6,8,15,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,5,14	2,6,8	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,5,14,16,17,18	2,6,8,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,5,14,18	2,6,8,15,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,5,14,16,17	2,6,8,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,17	2,6,8,13,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,5,16,18	2,6,8,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,17,18	2,6,8,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,5,16	2,6,8,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,5,14,18	2,6,8,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,5,14,16,17	2,6,8,13,17	2^{-1}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,5,14	2,6,8,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,5,14,16,17,18	2,6,8,13,15,17,18	2^{-1}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,5,12	2,6,8	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,5,12,16,17,18	2,6,8,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,5,12,18	2,6,8,15,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,5,12,16,17	2,6,8,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,5,12,14,17,18	2,6,8,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,12,14,16	2,6,8	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,5,12,14,17	2,6,8,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,12,14,16,18	2,6,8,15,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,5,12,18	2,6,8,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,5,12,16,17	2,6,8,13,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,5,12	2,6,8,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,5,12,16,17,18	2,6,8,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,5,12,14,17	2,6,8,13,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,5,12,14,16,18	2,6,8,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,5,12,14,17,18	2,6,8,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,5,12,14,16	2,6,8,13,15	$2^{-17.5}$

Table 0.1642 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,5,17	2,6,8,11,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,5,16,18	2,6,8,11,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,5,17,18	2,6,8,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,5,16	2,6,8,11,15	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,5,14,18	2,6,8,11,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,5,14,16,17	2,6,8,11,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,5,14	2,6,8,11,15	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,5,14,16,17,18	2,6,8,11,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,5,17,18	2,6,8,11,13,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,5,16	2,6,8,11,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,5,17	2,6,8,11,13,15,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,16,18	2,6,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,5,14	2,6,8,11,13	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,5,14,16,17,18	2,6,8,11,13,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,5,14,18	2,6,8,11,13,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,5,14,16,17	2,6,8,11,13,15,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,5,12,18	2,6,8,11,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,5,12,16,17	2,6,8,11,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,5,12	2,6,8,11,15	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,5,12,16,17,18	2,6,8,11,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,5,12,14,17	2,6,8,11,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,5,12,14,16,18	2,6,8,11,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,5,12,14,17,18	2,6,8,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,5,12,14,16	2,6,8,11,15	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,5,12	2,6,8,11,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,12,16,17,18	2,6,8,11,13,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,5,12,18	2,6,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,12,16,17	2,6,8,11,13,15,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,5,12,14,17,18	2,6,8,11,13,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,5,12,14,16	2,6,8,11,13	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,5,12,14,17	2,6,8,11,13,15,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,5,12,14,16,18	2,6,8,11,13,15,18	$2^{-6.5}$

Table 0.1643 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,5,10	2,6,8	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,5,10,16,17,18	2,6,8,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,5,10,18	2,6,8,15,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,5,10,16,17	2,6,8,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,5,10,14,17,18	2,6,8,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,5,10,14,16	2,6,8	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,5,10,14,17	2,6,8,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,5,10,14,16,18	2,6,8,15,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,5,10,18	2,6,8,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,5,10,16,17	2,6,8,13,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,5,10	2,6,8,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,5,10,16,17,18	2,6,8,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,5,10,14,17	2,6,8,13,17	2^{-34}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,5,10,14,16,18	2,6,8,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,5,10,14,17,18	2,6,8,13,15,17,18	2^{-34}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,5,10,14,16	2,6,8,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,10,12,17,18	2,6,8,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,10,12,16	2,6,8	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,10,12,17	2,6,8,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,10,12,16,18	2,6,8,15,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,5,10,12,14	2,6,8	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,5,10,12,14,16,17,18	2,6,8,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,5,10,12,14,18	2,6,8,15,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,10,12,14,16,17	2,6,8,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,5,10,12,17	2,6,8,13,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,5,10,12,16,18	2,6,8,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,5,10,12,17,18	2,6,8,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,5,10,12,16	2,6,8,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,5,10,12,14,18	2,6,8,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,5,10,12,14,16,17	2,6,8,13,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,5,10,12,14	2,6,8,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,5,10,12,14,16,17,18	2,6,8,13,15,17,18	2^{-12}

Table 0.1644 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,5,10,18	2,6,8,11,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,5,10,16,17	2,6,8,11,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,5,10	2,6,8,11,15	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,5,10,16,17,18	2,6,8,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,5,10,14,17	2,6,8,11,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,5,10,14,16,18	2,6,8,11,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,5,10,14,17,18	2,6,8,11,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,5,10,14,16	2,6,8,11,15	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,10	2,6,8,11,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,5,10,16,17,18	2,6,8,11,13,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,10,18	2,6,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,5,10,16,17	2,6,8,11,13,15,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,5,10,14,17,18	2,6,8,11,13,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,5,10,14,16	2,6,8,11,13	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,5,10,14,17	2,6,8,11,13,15,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,5,10,14,16,18	2,6,8,11,13,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,5,10,12,17	2,6,8,11,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,5,10,12,16,18	2,6,8,11,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,5,10,12,17,18	2,6,8,11,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,5,10,12,16	2,6,8,11,15	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,5,10,12,14,18	2,6,8,11,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,5,10,12,14,16,17	2,6,8,11,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,5,10,12,14	2,6,8,11,15	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,5,10,12,14,16,17,18	2,6,8,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,5,10,12,17,18	2,6,8,11,13,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,5,10,12,16	2,6,8,11,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,5,10,12,17	2,6,8,11,13,15,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,5,10,12,16,18	2,6,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,5,10,12,14	2,6,8,11,13	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,5,10,12,14,16,17,18	2,6,8,11,13,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,5,10,12,14,18	2,6,8,11,13,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,5,10,12,14,16,17	2,6,8,11,13,15,17	2^{-23}

Table 0.1645 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,5,17	2,6,8,9,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,5,16,18	2,6,8,9,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,5,17,18	2,6,8,9,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,5,16	2,6,8,9,15	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,5,14,18	2,6,8,9,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,5,14,16,17	2,6,8,9,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,5,14	2,6,8,9,15	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,5,14,16,17,18	2,6,8,9,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,5,17,18	2,6,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,5,16	2,6,8,9,13	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,5,17	2,6,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,5,16,18	2,6,8,9,13,15,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,5,14	2,6,8,9,13	2^{-34}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,5,14,16,17,18	2,6,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,5,14,18	2,6,8,9,13,15,18	2^{-34}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,5,14,16,17	2,6,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,12,18	2,6,8,9,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,5,12,16,17	2,6,8,9,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,12	2,6,8,9,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,5,12,16,17,18	2,6,8,9,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,5,12,14,17	2,6,8,9,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,5,12,14,16,18	2,6,8,9,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,5,12,14,17,18	2,6,8,9,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,5,12,14,16	2,6,8,9,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,5,12	2,6,8,9,13	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,5,12,16,17,18	2,6,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,5,12,18	2,6,8,9,13,15,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,5,12,16,17	2,6,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,5,12,14,17,18	2,6,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,5,12,14,16	2,6,8,9,13	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,5,12,14,17	2,6,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,5,12,14,16,18	2,6,8,9,13,15,18	2^{-12}

Table 0.1646 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,5,17,18	2,6,8,9,11,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,5,16	2,6,8,9,11	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,5,17	2,6,8,9,11,15,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,5,16,18	2,6,8,9,11,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,5,14	2,6,8,9,11	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,5,14,16,17,18	2,6,8,9,11,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,5,14,18	2,6,8,9,11,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,5,14,16,17	2,6,8,9,11,15,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,5,17	2,6,8,9,11,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,5,16,18	2,6,8,9,11,13,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,5,17,18	2,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,5,16	2,6,8,9,11,13,15	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,5,14,18	2,6,8,9,11,13,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,5,14,16,17	2,6,8,9,11,13,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,5,14	2,6,8,9,11,13,15	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,5,14,16,17,18	2,6,8,9,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,12	2,6,8,9,11	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,5,12,16,17,18	2,6,8,9,11,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,12,18	2,6,8,9,11,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,5,12,16,17	2,6,8,9,11,15,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,5,12,14,17,18	2,6,8,9,11,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,5,12,14,16	2,6,8,9,11	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,5,12,14,17	2,6,8,9,11,15,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,5,12,14,16,18	2,6,8,9,11,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,5,12,18	2,6,8,9,11,13,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,5,12,16,17	2,6,8,9,11,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,5,12	2,6,8,9,11,13,15	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,5,12,16,17,18	2,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,5,12,14,17	2,6,8,9,11,13,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,12,14,16,18	2,6,8,9,11,13,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,5,12,14,17,18	2,6,8,9,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,12,14,16	2,6,8,9,11,13,15	2^{-23}

Table 0.1647 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,5,10,18	2,6,8,9,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,5,10,16,17	2,6,8,9,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,5,10	2,6,8,9,15	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,5,10,16,17,18	2,6,8,9,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,5,10,14,17	2,6,8,9,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,5,10,14,16,18	2,6,8,9,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,5,10,14,17,18	2,6,8,9,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,5,10,14,16	2,6,8,9,15	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,5,10	2,6,8,9,13	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,5,10,16,17,18	2,6,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,5,10,18	2,6,8,9,13,15,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,5,10,16,17	2,6,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,5,10,14,17,18	2,6,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,5,10,14,16	2,6,8,9,13	2^{-1}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,5,10,14,17	2,6,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,5,10,14,16,18	2,6,8,9,13,15,18	2^{-1}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,5,10,12,17	2,6,8,9,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,5,10,12,16,18	2,6,8,9,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,5,10,12,17,18	2,6,8,9,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,5,10,12,16	2,6,8,9,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,5,10,12,14,18	2,6,8,9,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,5,10,12,14,16,17	2,6,8,9,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,5,10,12,14	2,6,8,9,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,5,10,12,14,16,17,18	2,6,8,9,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,5,10,12,17,18	2,6,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,5,10,12,16	2,6,8,9,13	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,5,10,12,17	2,6,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,5,10,12,16,18	2,6,8,9,13,15,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,5,10,12,14	2,6,8,9,13	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,5,10,12,14,16,17,18	2,6,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,5,10,12,14,18	2,6,8,9,13,15,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,5,10,12,14,16,17	2,6,8,9,13,15,17	$2^{-17.5}$

Table 0.1648 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,5,10	2,6,8,9,11	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,10,16,17,18	2,6,8,9,11,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,5,10,18	2,6,8,9,11,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,5,10,16,17	2,6,8,9,11,15,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,5,10,14,17,18	2,6,8,9,11,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,5,10,14,16	2,6,8,9,11	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,5,10,14,17	2,6,8,9,11,15,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,5,10,14,16,18	2,6,8,9,11,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,5,10,18	2,6,8,9,11,13,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,10,16,17	2,6,8,9,11,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,5,10	2,6,8,9,11,13,15	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,5,10,16,17,18	2,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,5,10,14,17	2,6,8,9,11,13,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,5,10,14,16,18	2,6,8,9,11,13,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,5,10,14,17,18	2,6,8,9,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,5,10,14,16	2,6,8,9,11,13,15	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,5,10,12,17,18	2,6,8,9,11,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,5,10,12,16	2,6,8,9,11	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,5,10,12,17	2,6,8,9,11,15,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,5,10,12,16,18	2,6,8,9,11,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,5,10,12,14	2,6,8,9,11	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,5,10,12,14,16,17,18	2,6,8,9,11,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,5,10,12,14,18	2,6,8,9,11,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,5,10,12,14,16,17	2,6,8,9,11,15,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,5,10,12,17	2,6,8,9,11,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,5,10,12,16,18	2,6,8,9,11,13,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,5,10,12,17,18	2,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,5,10,12,16	2,6,8,9,11,13,15	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,5,10,12,14,18	2,6,8,9,11,13,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,5,10,12,14,16,17	2,6,8,9,11,13,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,5,10,12,14	2,6,8,9,11,13,15	2^{-12}
$(1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,5,10,12,14,16,17,18	2,6,8,9,11,13,15,17,18	$2^{-6.5}$

Table 0.1649 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,5,7,18	2,6,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,5,7,16,17	2,6,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,5,7	2,6,15	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,5,7,16,17,18	2,6,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,5,7,14,17	2,6,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,5,7,14,16,18	2,6,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,5,7,14,17,18	2,6,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,5,7,14,16	2,6,15	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,5,7	2,6,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,7,16,17,18	2,6,13,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,5,7,18	2,6,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,7,16,17	2,6,13,15,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,5,7,14,17,18	2,6,13,17,18	2^{-1}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,5,7,14,16	2,6,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,5,7,14,17	2,6,13,15,17	2^{-1}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,5,7,14,16,18	2,6,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,5,7,12,17	2,6,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,5,7,12,16,18	2,6,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,5,7,12,17,18	2,6,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,5,7,12,16	2,6,15	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,5,7,12,14,18	2,6,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,5,7,12,14,16,17	2,6,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,5,7,12,14	2,6,15	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,5,7,12,14,16,17,18	2,6,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,5,7,12,17,18	2,6,13,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,5,7,12,16	2,6,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,5,7,12,17	2,6,13,15,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,5,7,12,16,18	2,6,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,5,7,12,14	2,6,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,7,12,14,16,17,18	2,6,13,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,5,7,12,14,18	2,6,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,7,12,14,16,17	2,6,13,15,17	2^{-23}

Table 0.1650 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,5,7	2,6,11	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,5,7,16,17,18	2,6,11,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,5,7,18	2,6,11,15,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,5,7,16,17	2,6,11,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,5,7,14,17,18	2,6,11,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,5,7,14,16	2,6,11	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,5,7,14,17	2,6,11,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,5,7,14,16,18	2,6,11,15,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,5,7,18	2,6,11,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,5,7,16,17	2,6,11,13,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,5,7	2,6,11,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,5,7,16,17,18	2,6,11,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,5,7,14,17	2,6,11,13,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1)$	1,5,7,14,16,18	2,6,11,13,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,5,7,14,17,18	2,6,11,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,5,7,14,16	2,6,11,13,15	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,12,17,18	2,6,11,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,12,16	2,6,11	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,12,17	2,6,11,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,12,16,18	2,6,11,15,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,12,14	2,6,11	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,5,7,12,14,16,17,18	2,6,11,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,12,14,18	2,6,11,15,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,5,7,12,14,16,17	2,6,11,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,12,17	2,6,11,13,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,5,7,12,16,18	2,6,11,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,12,17,18	2,6,11,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,5,7,12,16	2,6,11,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,5,7,12,14,18	2,6,11,13,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,5,7,12,14,16,17	2,6,11,13,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,5,7,12,14	2,6,11,13,15	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,5,7,12,14,16,17,18	2,6,11,13,15,17,18	2^{-12}

Table 0.1651 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,5,7,10,17	2,6,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,5,7,10,16,18	2,6,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,5,7,10,17,18	2,6,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,5,7,10,16	2,6,15	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,5,7,10,14,18	2,6,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,5,7,10,14,16,17	2,6,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,5,7,10,14	2,6,15	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,5,7,10,14,16,17,18	2,6,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,5,7,10,17,18	2,6,13,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,5,7,10,16	2,6,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,5,7,10,17	2,6,13,15,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,5,7,10,16,18	2,6,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,5,7,10,14	2,6,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,5,7,10,14,16,17,18	2,6,13,17,18	2^{-34}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,5,7,10,14,18	2,6,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,5,7,10,14,16,17	2,6,13,15,17	2^{-34}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,5,7,10,12,18	2,6,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,5,7,10,12,16,17	2,6,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,5,7,10,12	2,6,15	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,5,7,10,12,16,17,18	2,6,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,5,7,10,12,14,17	2,6,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,5,7,10,12,14,16,18	2,6,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,5,7,10,12,14,17,18	2,6,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,5,7,10,12,14,16	2,6,15	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,7,10,12	2,6,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,5,7,10,12,16,17,18	2,6,13,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,7,10,12,18	2,6,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,5,7,10,12,16,17	2,6,13,15,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,5,7,10,12,14,17,18	2,6,13,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,5,7,10,12,14,16	2,6,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,5,7,10,12,14,17	2,6,13,15,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,5,7,10,12,14,16,18	2,6,13,15,18	$2^{-17.5}$

Table 0.1652 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,10,17,18	2,6,11,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,10,16	2,6,11	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,10,17	2,6,11,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,10,16,18	2,6,11,15,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,5,7,10,14	2,6,11	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,5,7,10,14,16,17,18	2,6,11,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,5,7,10,14,18	2,6,11,15,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,5,7,10,14,16,17	2,6,11,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,5,7,10,17	2,6,11,13,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,7,10,16,18	2,6,11,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,5,7,10,17,18	2,6,11,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,7,10,16	2,6,11,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,5,7,10,14,18	2,6,11,13,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,5,7,10,14,16,17	2,6,11,13,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,5,7,10,14	2,6,11,13,15	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,5,7,10,14,16,17,18	2,6,11,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,5,7,10,12	2,6,11	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,5,7,10,12,16,17,18	2,6,11,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,5,7,10,12,18	2,6,11,15,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,5,7,10,12,16,17	2,6,11,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,10,12,14,17,18	2,6,11,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,5,7,10,12,14,16	2,6,11	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,10,12,14,17	2,6,11,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,5,7,10,12,14,16,18	2,6,11,15,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,5,7,10,12,18	2,6,11,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,5,7,10,12,16,17	2,6,11,13,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,5,7,10,12	2,6,11,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,5,7,10,12,16,17,18	2,6,11,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,5,7,10,12,14,17	2,6,11,13,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,5,7,10,12,14,16,18	2,6,11,13,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,5,7,10,12,14,17,18	2,6,11,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,5,7,10,12,14,16	2,6,11,13,15	$2^{-28.5}$

Table 0.1653 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,5,7	2,6,9	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,5,7,16,17,18	2,6,9,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,7,18	2,6,9,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,5,7,16,17	2,6,9,15,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,5,7,14,17,18	2,6,9,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,5,7,14,16	2,6,9	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,5,7,14,17	2,6,9,15,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,5,7,14,16,18	2,6,9,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,5,7,18	2,6,9,13,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,5,7,16,17	2,6,9,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,5,7	2,6,9,13,15	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,5,7,16,17,18	2,6,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,5,7,14,17	2,6,9,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,5,7,14,16,18	2,6,9,13,18	2^{-34}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,5,7,14,17,18	2,6,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,5,7,14,16	2,6,9,13,15	2^{-34}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,5,7,12,17,18	2,6,9,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,5,7,12,16	2,6,9	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,5,7,12,17	2,6,9,15,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,5,7,12,16,18	2,6,9,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,5,7,12,14	2,6,9	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,5,7,12,14,16,17,18	2,6,9,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,5,7,12,14,18	2,6,9,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,5,7,12,14,16,17	2,6,9,15,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,5,7,12,17	2,6,9,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,5,7,12,16,18	2,6,9,13,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,5,7,12,17,18	2,6,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,5,7,12,16	2,6,9,13,15	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,5,7,12,14,18	2,6,9,13,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,5,7,12,14,16,17	2,6,9,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,5,7,12,14	2,6,9,13,15	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,5,7,12,14,16,17,18	2,6,9,13,15,17,18	$2^{-17.5}$

Table 0.1654 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,5,7,18	2,6,9,11,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,5,7,16,17	2,6,9,11,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,5,7	2,6,9,11,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,5,7,16,17,18	2,6,9,11,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,14,17	2,6,9,11,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,5,7,14,16,18	2,6,9,11,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,14,17,18	2,6,9,11,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,5,7,14,16	2,6,9,11,15	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,5,7	2,6,9,11,13	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,5,7,16,17,18	2,6,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,5,7,18	2,6,9,11,13,15,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,5,7,16,17	2,6,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,5,7,14,17,18	2,6,9,11,13,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,5,7,14,16	2,6,9,11,13	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,5,7,14,17	2,6,9,11,13,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,5,7,14,16,18	2,6,9,11,13,15,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,5,7,12,17	2,6,9,11,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,5,7,12,16,18	2,6,9,11,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,5,7,12,17,18	2,6,9,11,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,5,7,12,16	2,6,9,11,15	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,5,7,12,14,18	2,6,9,11,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0)$	1,5,7,12,14,16,17	2,6,9,11,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,5,7,12,14	2,6,9,11,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,5,7,12,14,16,17,18	2,6,9,11,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,5,7,12,17,18	2,6,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,5,7,12,16	2,6,9,11,13	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,5,7,12,17	2,6,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,5,7,12,16,18	2,6,9,11,13,15,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,5,7,12,14	2,6,9,11,13	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,5,7,12,14,16,17,18	2,6,9,11,13,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,5,7,12,14,18	2,6,9,11,13,15,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,5,7,12,14,16,17	2,6,9,11,13,15,17	$2^{-28.5}$

Table 0.1655 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,5,7,10,17,18	2,6,9,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,5,7,10,16	2,6,9	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,5,7,10,17	2,6,9,15,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,5,7,10,16,18	2,6,9,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,5,7,10,14	2,6,9	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,5,7,10,14,16,17,18	2,6,9,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,5,7,10,14,18	2,6,9,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,5,7,10,14,16,17	2,6,9,15,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,5,7,10,17	2,6,9,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,5,7,10,16,18	2,6,9,13,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,5,7,10,17,18	2,6,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,5,7,10,16	2,6,9,13,15	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,5,7,10,14,18	2,6,9,13,18	2^{-1}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,5,7,10,14,16,17	2,6,9,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,5,7,10,14	2,6,9,13,15	2^{-1}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,5,7,10,14,16,17,18	2,6,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,5,7,10,12	2,6,9	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,7,10,12,16,17,18	2,6,9,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,5,7,10,12,18	2,6,9,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,7,10,12,16,17	2,6,9,15,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,5,7,10,12,14,17,18	2,6,9,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,5,7,10,12,14,16	2,6,9	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,5,7,10,12,14,17	2,6,9,15,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,5,7,10,12,14,16,18	2,6,9,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,5,7,10,12,18	2,6,9,13,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,5,7,10,12,16,17	2,6,9,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,5,7,10,12	2,6,9,13,15	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,5,7,10,12,16,17,18	2,6,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,10,12,14,17	2,6,9,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,5,7,10,12,14,16,18	2,6,9,13,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,10,12,14,17,18	2,6,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,5,7,10,12,14,16	2,6,9,13,15	2^{-23}

Table 0.1656 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,5,7,10,17	2,6,9,11,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,5,7,10,16,18	2,6,9,11,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,5,7,10,17,18	2,6,9,11,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,5,7,10,16	2,6,9,11,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,5,7,10,14,18	2,6,9,11,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,5,7,10,14,16,17	2,6,9,11,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,5,7,10,14	2,6,9,11,15	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,5,7,10,14,16,17,18	2,6,9,11,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,5,7,10,17,18	2,6,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,5,7,10,16	2,6,9,11,13	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,5,7,10,17	2,6,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,5,7,10,16,18	2,6,9,11,13,15,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,5,7,10,14	2,6,9,11,13	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,5,7,10,14,16,17,18	2,6,9,11,13,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,5,7,10,14,18	2,6,9,11,13,15,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,5,7,10,14,16,17	2,6,9,11,13,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,5,7,10,12,18	2,6,9,11,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,7,10,12,16,17	2,6,9,11,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,5,7,10,12	2,6,9,11,15	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,7,10,12,16,17,18	2,6,9,11,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,5,7,10,12,14,17	2,6,9,11,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,5,7,10,12,14,16,18	2,6,9,11,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,5,7,10,12,14,17,18	2,6,9,11,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,5,7,10,12,14,16	2,6,9,11,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,5,7,10,12	2,6,9,11,13	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,5,7,10,12,16,17,18	2,6,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,5,7,10,12,18	2,6,9,11,13,15,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,5,7,10,12,16,17	2,6,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,5,7,10,12,14,17,18	2,6,9,11,13,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,5,7,10,12,14,16	2,6,9,11,13	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,5,7,10,12,14,17	2,6,9,11,13,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,5,7,10,12,14,16,18	2,6,9,11,13,15,18	2^{-12}

Table 0.1657 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,5,7,17	2,6,8,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,5,7,16,18	2,6,8,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,5,7,17,18	2,6,8,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,5,7,16	2,6,8,15	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,5,7,14,18	2,6,8,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,5,7,14,16,17	2,6,8,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,5,7,14	2,6,8,15	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,5,7,14,16,17,18	2,6,8,15,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,5,7,17,18	2,6,8,13,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,5,7,16	2,6,8,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,5,7,17	2,6,8,13,15,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,5,7,16,18	2,6,8,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,5,7,14	2,6,8,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,5,7,14,16,17,18	2,6,8,13,17,18	2^{-1}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,5,7,14,18	2,6,8,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,5,7,14,16,17	2,6,8,13,15,17	2^{-1}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,7,12,18	2,6,8,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,5,7,12,16,17	2,6,8,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,7,12	2,6,8,15	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,5,7,12,16,17,18	2,6,8,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,5,7,12,14,17	2,6,8,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,5,7,12,14,16,18	2,6,8,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,5,7,12,14,17,18	2,6,8,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,5,7,12,14,16	2,6,8,15	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,5,7,12	2,6,8,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,5,7,12,16,17,18	2,6,8,13,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,5,7,12,18	2,6,8,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,5,7,12,16,17	2,6,8,13,15,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,5,7,12,14,17,18	2,6,8,13,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,12,14,16	2,6,8,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,5,7,12,14,17	2,6,8,13,15,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,12,14,16,18	2,6,8,13,15,18	$2^{-17.5}$

Table 0.1658 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,5,7,17,18	2,6,8,11,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,5,7,16	2,6,8,11	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,5,7,17	2,6,8,11,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,5,7,16,18	2,6,8,11,15,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,5,7,14	2,6,8,11	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,5,7,14,16,17,18	2,6,8,11,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,5,7,14,18	2,6,8,11,15,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,5,7,14,16,17	2,6,8,11,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,5,7,17	2,6,8,11,13,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,5,7,16,18	2,6,8,11,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,5,7,17,18	2,6,8,11,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,5,7,16	2,6,8,11,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,5,7,14,18	2,6,8,11,13,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,5,7,14,16,17	2,6,8,11,13,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,5,7,14	2,6,8,11,13,15	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,5,7,14,16,17,18	2,6,8,11,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,7,12	2,6,8,11	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,5,7,12,16,17,18	2,6,8,11,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,7,12,18	2,6,8,11,15,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,5,7,12,16,17	2,6,8,11,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,5,7,12,14,17,18	2,6,8,11,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,5,7,12,14,16	2,6,8,11	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,5,7,12,14,17	2,6,8,11,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,5,7,12,14,16,18	2,6,8,11,15,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,5,7,12,18	2,6,8,11,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,5,7,12,16,17	2,6,8,11,13,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,5,7,12	2,6,8,11,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,5,7,12,16,17,18	2,6,8,11,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,5,7,12,14,17	2,6,8,11,13,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,5,7,12,14,16,18	2,6,8,11,13,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,5,7,12,14,17,18	2,6,8,11,13,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,5,7,12,14,16	2,6,8,11,13,15	$2^{-6.5}$

Table 0.1659 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,5,7,10,18	2,6,8,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,5,7,10,16,17	2,6,8,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,5,7,10	2,6,8,15	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,5,7,10,16,17,18	2,6,8,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,5,7,10,14,17	2,6,8,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,5,7,10,14,16,18	2,6,8,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,5,7,10,14,17,18	2,6,8,15,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,5,7,10,14,16	2,6,8,15	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,5,7,10	2,6,8,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,5,7,10,16,17,18	2,6,8,13,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,5,7,10,18	2,6,8,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,5,7,10,16,17	2,6,8,13,15,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,5,7,10,14,17,18	2,6,8,13,17,18	2^{-34}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,5,7,10,14,16	2,6,8,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,5,7,10,14,17	2,6,8,13,15,17	2^{-34}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,5,7,10,14,16,18	2,6,8,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,5,7,10,12,17	2,6,8,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,5,7,10,12,16,18	2,6,8,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,5,7,10,12,17,18	2,6,8,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,5,7,10,12,16	2,6,8,15	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,5,7,10,12,14,18	2,6,8,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,5,7,10,12,14,16,17	2,6,8,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,5,7,10,12,14	2,6,8,15	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,5,7,10,12,14,16,17,18	2,6,8,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,5,7,10,12,17,18	2,6,8,13,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,5,7,10,12,16	2,6,8,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,5,7,10,12,17	2,6,8,13,15,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,5,7,10,12,16,18	2,6,8,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,5,7,10,12,14	2,6,8,13	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,5,7,10,12,14,16,17,18	2,6,8,13,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,5,7,10,12,14,18	2,6,8,13,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,5,7,10,12,14,16,17	2,6,8,13,15,17	2^{-12}

Table 0.1660 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,5,7,10	2,6,8,11	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,5,7,10,16,17,18	2,6,8,11,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,5,7,10,18	2,6,8,11,15,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,5,7,10,16,17	2,6,8,11,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,5,7,10,14,17,18	2,6,8,11,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,10,14,16	2,6,8,11	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,5,7,10,14,17	2,6,8,11,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,10,14,16,18	2,6,8,11,15,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,5,7,10,18	2,6,8,11,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,5,7,10,16,17	2,6,8,11,13,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,5,7,10	2,6,8,11,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,5,7,10,16,17,18	2,6,8,11,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,5,7,10,14,17	2,6,8,11,13,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,5,7,10,14,16,18	2,6,8,11,13,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,5,7,10,14,17,18	2,6,8,11,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,5,7,10,14,16	2,6,8,11,13,15	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,5,7,10,12,17,18	2,6,8,11,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,5,7,10,12,16	2,6,8,11	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,5,7,10,12,17	2,6,8,11,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,5,7,10,12,16,18	2,6,8,11,15,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,5,7,10,12,14	2,6,8,11	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,5,7,10,12,14,16,17,18	2,6,8,11,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,5,7,10,12,14,18	2,6,8,11,15,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,5,7,10,12,14,16,17	2,6,8,11,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,5,7,10,12,17	2,6,8,11,13,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,5,7,10,12,16,18	2,6,8,11,13,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,5,7,10,12,17,18	2,6,8,11,13,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,5,7,10,12,16	2,6,8,11,13,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,5,7,10,12,14,18	2,6,8,11,13,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,5,7,10,12,14,16,17	2,6,8,11,13,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,5,7,10,12,14	2,6,8,11,13,15	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,5,7,10,12,14,16,17,18	2,6,8,11,13,15,17,18	2^{-23}

Table 0.1661 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,5,7,17,18	2,6,8,9,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,5,7,16	2,6,8,9	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,5,7,17	2,6,8,9,15,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,5,7,16,18	2,6,8,9,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,5,7,14	2,6,8,9	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,5,7,14,16,17,18	2,6,8,9,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,5,7,14,18	2,6,8,9,15,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,5,7,14,16,17	2,6,8,9,15,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,5,7,17	2,6,8,9,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,16,18	2,6,8,9,13,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,5,7,17,18	2,6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,16	2,6,8,9,13,15	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,5,7,14,18	2,6,8,9,13,18	2^{-34}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,5,7,14,16,17	2,6,8,9,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,5,7,14	2,6,8,9,13,15	2^{-34}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,5,7,14,16,17,18	2,6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,5,7,12	2,6,8,9	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,5,7,12,16,17,18	2,6,8,9,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,5,7,12,18	2,6,8,9,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,5,7,12,16,17	2,6,8,9,15,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,5,7,12,14,17,18	2,6,8,9,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,5,7,12,14,16	2,6,8,9	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,5,7,12,14,17	2,6,8,9,15,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,5,7,12,14,16,18	2,6,8,9,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,5,7,12,18	2,6,8,9,13,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,7,12,16,17	2,6,8,9,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,5,7,12	2,6,8,9,13,15	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,7,12,16,17,18	2,6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,5,7,12,14,17	2,6,8,9,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,5,7,12,14,16,18	2,6,8,9,13,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,5,7,12,14,17,18	2,6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,5,7,12,14,16	2,6,8,9,13,15	2^{-12}

Table 0.1662 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,17	2,6,8,9,11,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,16,18	2,6,8,9,11,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,17,18	2,6,8,9,11,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,16	2,6,8,9,11,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,5,7,14,18	2,6,8,9,11,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,5,7,14,16,17	2,6,8,9,11,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,5,7,14	2,6,8,9,11,15	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,5,7,14,16,17,18	2,6,8,9,11,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,7,17,18	2,6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,5,7,16	2,6,8,9,11,13	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,7,17	2,6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,5,7,16,18	2,6,8,9,11,13,15,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,5,7,14	2,6,8,9,11,13	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,5,7,14,16,17,18	2,6,8,9,11,13,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,5,7,14,18	2,6,8,9,11,13,15,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,5,7,14,16,17	2,6,8,9,11,13,15,17	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,5,7,12,18	2,6,8,9,11,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,5,7,12,16,17	2,6,8,9,11,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,5,7,12	2,6,8,9,11,15	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,5,7,12,16,17,18	2,6,8,9,11,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,5,7,12,14,17	2,6,8,9,11,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,12,14,16,18	2,6,8,9,11,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,5,7,12,14,17,18	2,6,8,9,11,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,12,14,16	2,6,8,9,11,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,5,7,12	2,6,8,9,11,13	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,5,7,12,16,17,18	2,6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,7,12,18	2,6,8,9,11,13,15,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,5,7,12,16,17	2,6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,5,7,12,14,17,18	2,6,8,9,11,13,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,12,14,16	2,6,8,9,11,13	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,5,7,12,14,17	2,6,8,9,11,13,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,5,7,12,14,16,18	2,6,8,9,11,13,15,18	2^{-23}

Table 0.1663 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,5,7,10	2,6,8,9	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,5,7,10,16,17,18	2,6,8,9,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,5,7,10,18	2,6,8,9,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,5,7,10,16,17	2,6,8,9,15,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,5,7,10,14,17,18	2,6,8,9,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,5,7,10,14,16	2,6,8,9	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,5,7,10,14,17	2,6,8,9,15,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,5,7,10,14,16,18	2,6,8,9,15,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,7,10,18	2,6,8,9,13,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,5,7,10,16,17	2,6,8,9,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,7,10	2,6,8,9,13,15	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,5,7,10,16,17,18	2,6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,5,7,10,14,17	2,6,8,9,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,5,7,10,14,16,18	2,6,8,9,13,18	2^{-1}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,5,7,10,14,17,18	2,6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,5,7,10,14,16	2,6,8,9,13,15	2^{-1}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,5,7,10,12,17,18	2,6,8,9,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,5,7,10,12,16	2,6,8,9	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,5,7,10,12,17	2,6,8,9,15,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,5,7,10,12,16,18	2,6,8,9,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,5,7,10,12,14	2,6,8,9	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,5,7,10,12,14,16,17,18	2,6,8,9,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,5,7,10,12,14,18	2,6,8,9,15,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,5,7,10,12,14,16,17	2,6,8,9,15,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,5,7,10,12,17	2,6,8,9,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,5,7,10,12,16,18	2,6,8,9,13,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,5,7,10,12,17,18	2,6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,5,7,10,12,16	2,6,8,9,13,15	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,7,10,12,14,18	2,6,8,9,13,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,5,7,10,12,14,16,17	2,6,8,9,13,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,5,7,10,12,14	2,6,8,9,13,15	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,5,7,10,12,14,16,17,18	2,6,8,9,13,15,17,18	$2^{-17.5}$

Table 0.1664 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,5,7,10,18	2,6,8,9,11,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,5,7,10,16,17	2,6,8,9,11,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,5,7,10	2,6,8,9,11,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,5,7,10,16,17,18	2,6,8,9,11,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,5,7,10,14,17	2,6,8,9,11,17	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,5,7,10,14,16,18	2,6,8,9,11,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,5,7,10,14,17,18	2,6,8,9,11,15,17,18	2^{-23}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,5,7,10,14,16	2,6,8,9,11,15	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,5,7,10	2,6,8,9,11,13	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,10,16,17,18	2,6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,5,7,10,18	2,6,8,9,11,13,15,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,10,16,17	2,6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,5,7,10,14,17,18	2,6,8,9,11,13,17,18	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,5,7,10,14,16	2,6,8,9,11,13	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,5,7,10,14,17	2,6,8,9,11,13,15,17	$2^{-28.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,5,7,10,14,16,18	2,6,8,9,11,13,15,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,10,12,17	2,6,8,9,11,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,10,12,16,18	2,6,8,9,11,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,10,12,17,18	2,6,8,9,11,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,10,12,16	2,6,8,9,11,15	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,5,7,10,12,14,18	2,6,8,9,11,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,10,12,14,16,17	2,6,8,9,11,17	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,5,7,10,12,14	2,6,8,9,11,15	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,10,12,14,16,17,18	2,6,8,9,11,15,17,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,5,7,10,12,17,18	2,6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,10,12,16	2,6,8,9,11,13	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,5,7,10,12,17	2,6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,10,12,16,18	2,6,8,9,11,13,15,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,5,7,10,12,14	2,6,8,9,11,13	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,5,7,10,12,14,16,17,18	2,6,8,9,11,13,17,18	$2^{-6.5}$
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,5,7,10,12,14,18	2,6,8,9,11,13,15,18	2^{-12}
$(1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,5,7,10,12,14,16,17	2,6,8,9,11,13,15,17	$2^{-6.5}$

Table 0.1665 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,18	2,4,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,16,17	2,4,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1	2,4,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,16,17,18	2,4,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,14,17	2,4,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,14,16,18	2,4,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,14,17,18	2,4,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,14,16	2,4,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0)$	1	2,4,13	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,16,17,18	2,4,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,18	2,4,13,15,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,16,17	2,4,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,14,17,18	2,4,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,14,16	2,4,13	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,14,17	2,4,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,14,16,18	2,4,13,15,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,12,17	2,4,17	2^{-1}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,12,16,18	2,4,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,12,17,18	2,4,15,17,18	2^{-1}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,12,16	2,4,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,12,14,18	2,4,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,12,14,16,17	2,4,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,12,14	2,4,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,12,14,16,17,18	2,4,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,12,17,18	2,4,13,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,12,16	2,4,13	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,12,17	2,4,13,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,12,16,18	2,4,13,15,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,12,14	2,4,13	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,12,14,16,17,18	2,4,13,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,12,14,18	2,4,13,15,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,12,14,16,17	2,4,13,15,17	$2^{-6.5}$

Table 0.1666 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1	2,4,11	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,16,17,18	2,4,11,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,18	2,4,11,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,16,17	2,4,11,15,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,14,17,18	2,4,11,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,14,16	2,4,11	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,14,17	2,4,11,15,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,14,16,18	2,4,11,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,18	2,4,11,13,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,16,17	2,4,11,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1	2,4,11,13,15	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,16,17,18	2,4,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,14,17	2,4,11,13,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,14,16,18	2,4,11,13,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,14,17,18	2,4,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,14,16	2,4,11,13,15	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,12,17,18	2,4,11,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,12,16	2,4,11	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,12,17	2,4,11,15,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,12,16,18	2,4,11,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,12,14	2,4,11	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,12,14,16,17,18	2,4,11,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,12,14,18	2,4,11,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,12,14,16,17	2,4,11,15,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,12,17	2,4,11,13,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,12,16,18	2,4,11,13,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,12,17,18	2,4,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,12,16	2,4,11,13,15	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,12,14,18	2,4,11,13,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,12,14,16,17	2,4,11,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,12,14	2,4,11,13,15	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,12,14,16,17,18	2,4,11,13,15,17,18	$2^{-17.5}$

Table 0.1667 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(2)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,10,17	2,4,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,10,16,18	2,4,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,10,17,18	2,4,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,10,16	2,4,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,10,14,18	2,4,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,10,14,16,17	2,4,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,10,14	2,4,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,10,14,16,17,18	2,4,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,10,17,18	2,4,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,10,16	2,4,13	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,10,17	2,4,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,10,16,18	2,4,13,15,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,10,14	2,4,13	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,10,14,16,17,18	2,4,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,10,14,18	2,4,13,15,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,10,14,16,17	2,4,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,10,12,18	2,4,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,10,12,16,17	2,4,17	2^{-34}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,10,12	2,4,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,10,12,16,17,18	2,4,15,17,18	2^{-34}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,10,12,14,17	2,4,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,10,12,14,16,18	2,4,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,10,12,14,17,18	2,4,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,10,12,14,16	2,4,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,10,12	2,4,13	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,10,12,16,17,18	2,4,13,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,10,12,18	2,4,13,15,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,10,12,16,17	2,4,13,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,10,12,14,17,18	2,4,13,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,10,12,14,16	2,4,13	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,10,12,14,17	2,4,13,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,10,12,14,16,18	2,4,13,15,18	2^{-23}

Table 0.1668 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,10,17,18	2,4,11,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,10,16	2,4,11	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,10,17	2,4,11,15,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,10,16,18	2,4,11,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,10,14	2,4,11	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,10,14,16,17,18	2,4,11,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,10,14,18	2,4,11,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,10,14,16,17	2,4,11,15,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,10,17	2,4,11,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,10,16,18	2,4,11,13,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,10,17,18	2,4,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,10,16	2,4,11,13,15	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,10,14,18	2,4,11,13,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,10,14,16,17	2,4,11,13,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,10,14	2,4,11,13,15	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,10,14,16,17,18	2,4,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,10,12	2,4,11	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,10,12,16,17,18	2,4,11,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,10,12,18	2,4,11,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,10,12,16,17	2,4,11,15,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,10,12,14,17,18	2,4,11,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,10,12,14,16	2,4,11	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,10,12,14,17	2,4,11,15,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,10,12,14,16,18	2,4,11,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,10,12,18	2,4,11,13,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,10,12,16,17	2,4,11,13,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,10,12	2,4,11,13,15	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,10,12,16,17,18	2,4,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,10,12,14,17	2,4,11,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,10,12,14,16,18	2,4,11,13,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,10,12,14,17,18	2,4,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,10,12,14,16	2,4,11,13,15	2^{-12}

Table 0.1669 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1	2,4,9	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,16,17,18	2,4,9,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,18	2,4,9,15,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,16,17	2,4,9,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,14,17,18	2,4,9,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,14,16	2,4,9	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,14,17	2,4,9,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,14,16,18	2,4,9,15,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,18	2,4,9,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,16,17	2,4,9,13,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1	2,4,9,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,16,17,18	2,4,9,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,14,17	2,4,9,13,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,14,16,18	2,4,9,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,14,17,18	2,4,9,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,14,16	2,4,9,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,12,17,18	2,4,9,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,12,16	2,4,9	2^{-34}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,12,17	2,4,9,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,12,16,18	2,4,9,15,18	2^{-34}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,12,14	2,4,9	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,12,14,16,17,18	2,4,9,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,12,14,18	2,4,9,15,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,12,14,16,17	2,4,9,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,12,17	2,4,9,13,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,12,16,18	2,4,9,13,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,12,17,18	2,4,9,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,12,16	2,4,9,13,15	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,12,14,18	2,4,9,13,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,12,14,16,17	2,4,9,13,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,12,14	2,4,9,13,15	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,12,14,16,17,18	2,4,9,13,15,17,18	2^{-23}

Table 0.1670 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,18	2,4,9,11,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,16,17	2,4,9,11,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1	2,4,9,11,15	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,16,17,18	2,4,9,11,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,14,17	2,4,9,11,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,14,16,18	2,4,9,11,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,14,17,18	2,4,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,14,16	2,4,9,11,15	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1	2,4,9,11,13	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,16,17,18	2,4,9,11,13,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,18	2,4,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,16,17	2,4,9,11,13,15,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,14,17,18	2,4,9,11,13,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,14,16	2,4,9,11,13	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,14,17	2,4,9,11,13,15,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,14,16,18	2,4,9,11,13,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,12,17	2,4,9,11,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,12,16,18	2,4,9,11,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,12,17,18	2,4,9,11,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,12,16	2,4,9,11,15	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,12,14,18	2,4,9,11,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,12,14,16,17	2,4,9,11,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,12,14	2,4,9,11,15	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,12,14,16,17,18	2,4,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,12,17,18	2,4,9,11,13,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,12,16	2,4,9,11,13	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,12,17	2,4,9,11,13,15,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,12,16,18	2,4,9,11,13,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,12,14	2,4,9,11,13	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,12,14,16,17,18	2,4,9,11,13,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,12,14,18	2,4,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,12,14,16,17	2,4,9,11,13,15,17	2^{-12}

Table 0.1671 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,10,17,18	2,4,9,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,10,16	2,4,9	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,10,17	2,4,9,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,10,16,18	2,4,9,15,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,10,14	2,4,9	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,10,14,16,17,18	2,4,9,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,10,14,18	2,4,9,15,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,10,14,16,17	2,4,9,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,10,17	2,4,9,13,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,10,16,18	2,4,9,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,10,17,18	2,4,9,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,10,16	2,4,9,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,10,14,18	2,4,9,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,10,14,16,17	2,4,9,13,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,10,14	2,4,9,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,10,14,16,17,18	2,4,9,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,10,12	2,4,9	2^{-1}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,10,12,16,17,18	2,4,9,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,10,12,18	2,4,9,15,18	2^{-1}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,10,12,16,17	2,4,9,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,10,12,14,17,18	2,4,9,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,10,12,14,16	2,4,9	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,10,12,14,17	2,4,9,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,10,12,14,16,18	2,4,9,15,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,10,12,18	2,4,9,13,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,10,12,16,17	2,4,9,13,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,10,12	2,4,9,13,15	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,10,12,16,17,18	2,4,9,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,10,12,14,17	2,4,9,13,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,10,12,14,16,18	2,4,9,13,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,10,12,14,17,18	2,4,9,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,10,12,14,16	2,4,9,13,15	$2^{-6.5}$

Table 0.1672 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,10,17	2,4,9,11,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,10,16,18	2,4,9,11,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,10,17,18	2,4,9,11,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,10,16	2,4,9,11,15	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,10,14,18	2,4,9,11,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,10,14,16,17	2,4,9,11,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,10,14	2,4,9,11,15	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,10,14,16,17,18	2,4,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,10,17,18	2,4,9,11,13,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,10,16	2,4,9,11,13	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,10,17	2,4,9,11,13,15,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,10,16,18	2,4,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,10,14	2,4,9,11,13	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,10,14,16,17,18	2,4,9,11,13,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,10,14,18	2,4,9,11,13,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,10,14,16,17	2,4,9,11,13,15,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,10,12,18	2,4,9,11,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,10,12,16,17	2,4,9,11,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,10,12	2,4,9,11,15	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,10,12,16,17,18	2,4,9,11,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,10,12,14,17	2,4,9,11,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,10,12,14,16,18	2,4,9,11,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,10,12,14,17,18	2,4,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,10,12,14,16	2,4,9,11,15	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,10,12	2,4,9,11,13	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,10,12,16,17,18	2,4,9,11,13,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,10,12,18	2,4,9,11,13,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,10,12,16,17	2,4,9,11,13,15,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,10,12,14,17,18	2,4,9,11,13,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,10,12,14,16	2,4,9,11,13	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,10,12,14,17	2,4,9,11,13,15,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,10,12,14,16,18	2,4,9,11,13,15,18	$2^{-17.5}$

Table 0.1673 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,17	2,4,8,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,16,18	2,4,8,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,17,18	2,4,8,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,16	2,4,8,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,14,18	2,4,8,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,14,16,17	2,4,8,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,14	2,4,8,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,14,16,17,18	2,4,8,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,17,18	2,4,8,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,16	2,4,8,13	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,17	2,4,8,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,16,18	2,4,8,13,15,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,14	2,4,8,13	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,14,16,17,18	2,4,8,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,14,18	2,4,8,13,15,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,14,16,17	2,4,8,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,12,18	2,4,8,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,12,16,17	2,4,8,17	2^{-1}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,12	2,4,8,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,12,16,17,18	2,4,8,15,17,18	2^{-1}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,12,14,17	2,4,8,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,12,14,16,18	2,4,8,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,12,14,17,18	2,4,8,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,12,14,16	2,4,8,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,12	2,4,8,13	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,12,16,17,18	2,4,8,13,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,12,18	2,4,8,13,15,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,12,16,17	2,4,8,13,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,12,14,17,18	2,4,8,13,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,12,14,16	2,4,8,13	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,12,14,17	2,4,8,13,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,12,14,16,18	2,4,8,13,15,18	2^{-12}

Table 0.1674 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,17,18	2,4,8,11,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,16	2,4,8,11	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,17	2,4,8,11,15,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,16,18	2,4,8,11,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,14	2,4,8,11	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,14,16,17,18	2,4,8,11,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,14,18	2,4,8,11,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,14,16,17	2,4,8,11,15,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,17	2,4,8,11,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,16,18	2,4,8,11,13,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,17,18	2,4,8,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,16	2,4,8,11,13,15	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,14,18	2,4,8,11,13,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,14,16,17	2,4,8,11,13,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,14	2,4,8,11,13,15	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,14,16,17,18	2,4,8,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,12	2,4,8,11	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,12,16,17,18	2,4,8,11,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,12,18	2,4,8,11,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,12,16,17	2,4,8,11,15,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,12,14,17,18	2,4,8,11,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,12,14,16	2,4,8,11	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,12,14,17	2,4,8,11,15,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,12,14,16,18	2,4,8,11,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,12,18	2,4,8,11,13,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,12,16,17	2,4,8,11,13,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,12	2,4,8,11,13,15	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,12,16,17,18	2,4,8,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,12,14,17	2,4,8,11,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,12,14,16,18	2,4,8,11,13,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,12,14,17,18	2,4,8,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,12,14,16	2,4,8,11,13,15	2^{-23}

Table 0.1675 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,10,18	2,4,8,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,10,16,17	2,4,8,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,10	2,4,8,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,10,16,17,18	2,4,8,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,10,14,17	2,4,8,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,10,14,16,18	2,4,8,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,10,14,17,18	2,4,8,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,10,14,16	2,4,8,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,10	2,4,8,13	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,10,16,17,18	2,4,8,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,10,18	2,4,8,13,15,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,10,16,17	2,4,8,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,10,14,17,18	2,4,8,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,10,14,16	2,4,8,13	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,10,14,17	2,4,8,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,10,14,16,18	2,4,8,13,15,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,10,12,17	2,4,8,17	2^{-34}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,10,12,16,18	2,4,8,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,10,12,17,18	2,4,8,15,17,18	2^{-34}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,10,12,16	2,4,8,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,10,12,14,18	2,4,8,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,10,12,14,16,17	2,4,8,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,10,12,14	2,4,8,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,10,12,14,16,17,18	2,4,8,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,10,12,17,18	2,4,8,13,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,10,12,16	2,4,8,13	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,10,12,17	2,4,8,13,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,10,12,16,18	2,4,8,13,15,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,10,12,14	2,4,8,13	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,10,12,14,16,17,18	2,4,8,13,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,10,12,14,18	2,4,8,13,15,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,10,12,14,16,17	2,4,8,13,15,17	$2^{-28.5}$

Table 0.1676 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,10	2,4,8,11	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,10,16,17,18	2,4,8,11,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,10,18	2,4,8,11,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,10,16,17	2,4,8,11,15,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,10,14,17,18	2,4,8,11,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,10,14,16	2,4,8,11	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,10,14,17	2,4,8,11,15,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,10,14,16,18	2,4,8,11,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,10,18	2,4,8,11,13,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,10,16,17	2,4,8,11,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,10	2,4,8,11,13,15	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,10,16,17,18	2,4,8,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,10,14,17	2,4,8,11,13,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,10,14,16,18	2,4,8,11,13,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,10,14,17,18	2,4,8,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,10,14,16	2,4,8,11,13,15	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,10,12,17,18	2,4,8,11,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,10,12,16	2,4,8,11	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,10,12,17	2,4,8,11,15,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,10,12,16,18	2,4,8,11,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,10,12,14	2,4,8,11	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,10,12,14,16,17,18	2,4,8,11,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,10,12,14,18	2,4,8,11,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,10,12,14,16,17	2,4,8,11,15,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,10,12,17	2,4,8,11,13,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,10,12,16,18	2,4,8,11,13,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,10,12,17,18	2,4,8,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,10,12,16	2,4,8,11,13,15	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,10,12,14,18	2,4,8,11,13,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,10,12,14,16,17	2,4,8,11,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,10,12,14	2,4,8,11,13,15	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,10,12,14,16,17,18	2,4,8,11,13,15,17,18	$2^{-17.5}$

Table 0.1677 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,17,18	2,4,8,9,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,16	2,4,8,9	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,17	2,4,8,9,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,16,18	2,4,8,9,15,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,14	2,4,8,9	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,14,16,17,18	2,4,8,9,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,14,18	2,4,8,9,15,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,14,16,17	2,4,8,9,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,17	2,4,8,9,13,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,16,18	2,4,8,9,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,17,18	2,4,8,9,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,16	2,4,8,9,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,14,18	2,4,8,9,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,14,16,17	2,4,8,9,13,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,14	2,4,8,9,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,14,16,17,18	2,4,8,9,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,12	2,4,8,9	2^{-34}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,12,16,17,18	2,4,8,9,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,12,18	2,4,8,9,15,18	2^{-34}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,12,16,17	2,4,8,9,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,12,14,17,18	2,4,8,9,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,12,14,16	2,4,8,9	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,12,14,17	2,4,8,9,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,12,14,16,18	2,4,8,9,15,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,12,18	2,4,8,9,13,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0)$	1,12,16,17	2,4,8,9,13,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,12	2,4,8,9,13,15	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,12,16,17,18	2,4,8,9,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,12,14,17	2,4,8,9,13,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,12,14,16,18	2,4,8,9,13,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,12,14,17,18	2,4,8,9,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,12,14,16	2,4,8,9,13,15	$2^{-28.5}$

Table 0.1678 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,17	2,4,8,9,11,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,16,18	2,4,8,9,11,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,17,18	2,4,8,9,11,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,16	2,4,8,9,11,15	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,14,18	2,4,8,9,11,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,14,16,17	2,4,8,9,11,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,14	2,4,8,9,11,15	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,14,16,17,18	2,4,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,17,18	2,4,8,9,11,13,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,16	2,4,8,9,11,13	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,17	2,4,8,9,11,13,15,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,16,18	2,4,8,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,14	2,4,8,9,11,13	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,14,16,17,18	2,4,8,9,11,13,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,14,18	2,4,8,9,11,13,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,14,16,17	2,4,8,9,11,13,15,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,12,18	2,4,8,9,11,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,12,16,17	2,4,8,9,11,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,12	2,4,8,9,11,15	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,12,16,17,18	2,4,8,9,11,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,12,14,17	2,4,8,9,11,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,12,14,16,18	2,4,8,9,11,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,12,14,17,18	2,4,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,12,14,16	2,4,8,9,11,15	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,12	2,4,8,9,11,13	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,12,16,17,18	2,4,8,9,11,13,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,12,18	2,4,8,9,11,13,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,12,16,17	2,4,8,9,11,13,15,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,12,14,17,18	2,4,8,9,11,13,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,12,14,16	2,4,8,9,11,13	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,12,14,17	2,4,8,9,11,13,15,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,12,14,16,18	2,4,8,9,11,13,15,18	$2^{-17.5}$

Table 0.1679 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,10	2,4,8,9	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,10,16,17,18	2,4,8,9,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,10,18	2,4,8,9,15,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,10,16,17	2,4,8,9,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,10,14,17,18	2,4,8,9,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,10,14,16	2,4,8,9	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,10,14,17	2,4,8,9,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,10,14,16,18	2,4,8,9,15,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,10,18	2,4,8,9,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,10,16,17	2,4,8,9,13,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,10	2,4,8,9,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,10,16,17,18	2,4,8,9,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,10,14,17	2,4,8,9,13,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,10,14,16,18	2,4,8,9,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,10,14,17,18	2,4,8,9,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,10,14,16	2,4,8,9,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,10,12,17,18	2,4,8,9,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,10,12,16	2,4,8,9	2^{-1}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,10,12,17	2,4,8,9,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,10,12,16,18	2,4,8,9,15,18	2^{-1}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,10,12,14	2,4,8,9	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,10,12,14,16,17,18	2,4,8,9,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,10,12,14,18	2,4,8,9,15,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,10,12,14,16,17	2,4,8,9,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,10,12,17	2,4,8,9,13,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,10,12,16,18	2,4,8,9,13,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,10,12,17,18	2,4,8,9,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,10,12,16	2,4,8,9,13,15	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,10,12,14,18	2,4,8,9,13,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,10,12,14,16,17	2,4,8,9,13,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,10,12,14	2,4,8,9,13,15	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,10,12,14,16,17,18	2,4,8,9,13,15,17,18	2^{-12}

Table 0.1680 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,10,18	2,4,8,9,11,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,10,16,17	2,4,8,9,11,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,10	2,4,8,9,11,15	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,10,16,17,18	2,4,8,9,11,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,10,14,17	2,4,8,9,11,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,10,14,16,18	2,4,8,9,11,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,10,14,17,18	2,4,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,10,14,16	2,4,8,9,11,15	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,10	2,4,8,9,11,13	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,10,16,17,18	2,4,8,9,11,13,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,10,18	2,4,8,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,10,16,17	2,4,8,9,11,13,15,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,10,14,17,18	2,4,8,9,11,13,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,10,14,16	2,4,8,9,11,13	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,10,14,17	2,4,8,9,11,13,15,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,10,14,16,18	2,4,8,9,11,13,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,10,12,17	2,4,8,9,11,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,10,12,16,18	2,4,8,9,11,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,10,12,17,18	2,4,8,9,11,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,10,12,16	2,4,8,9,11,15	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,10,12,14,18	2,4,8,9,11,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,10,12,14,16,17	2,4,8,9,11,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,10,12,14	2,4,8,9,11,15	2^{-12}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,10,12,14,16,17,18	2,4,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,10,12,17,18	2,4,8,9,11,13,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,10,12,16	2,4,8,9,11,13	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,10,12,17	2,4,8,9,11,13,15,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,10,12,16,18	2,4,8,9,11,13,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,10,12,14	2,4,8,9,11,13	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,10,12,14,16,17,18	2,4,8,9,11,13,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,10,12,14,18	2,4,8,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,10,12,14,16,17	2,4,8,9,11,13,15,17	2^{-23}

Table 0.1681 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,7	2,4	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,7,16,17,18	2,4,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,7,18	2,4,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,7,16,17	2,4,15,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,7,14,17,18	2,4,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,7,14,16	2,4	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,7,14,17	2,4,15,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,7,14,16,18	2,4,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,7,18	2,4,13,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,7,16,17	2,4,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,7	2,4,13,15	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,7,16,17,18	2,4,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,7,14,17	2,4,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,7,14,16,18	2,4,13,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,7,14,17,18	2,4,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,7,14,16	2,4,13,15	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,7,12,17,18	2,4,17,18	2^{-1}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,7,12,16	2,4	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,7,12,17	2,4,15,17	2^{-1}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,7,12,16,18	2,4,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,7,12,14	2,4	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1)$	1,7,12,14,16,17,18	2,4,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0)$	1,7,12,14,18	2,4,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$	1,7,12,14,16,17	2,4,15,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,7,12,17	2,4,13,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,7,12,16,18	2,4,13,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,7,12,17,18	2,4,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,7,12,16	2,4,13,15	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,7,12,14,18	2,4,13,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,7,12,14,16,17	2,4,13,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,7,12,14	2,4,13,15	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,7,12,14,16,17,18	2,4,13,15,17,18	$2^{-6.5}$

Table 0.1682 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,7,18	2,4,11,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,7,16,17	2,4,11,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,7	2,4,11,15	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,7,16,17,18	2,4,11,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,7,14,17	2,4,11,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,7,14,16,18	2,4,11,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,7,14,17,18	2,4,11,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,7,14,16	2,4,11,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,7	2,4,11,13	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,7,16,17,18	2,4,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,7,18	2,4,11,13,15,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,7,16,17	2,4,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,7,14,17,18	2,4,11,13,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,7,14,16	2,4,11,13	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,7,14,17	2,4,11,13,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,7,14,16,18	2,4,11,13,15,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,7,12,17	2,4,11,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,7,12,16,18	2,4,11,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,7,12,17,18	2,4,11,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,7,12,16	2,4,11,15	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,7,12,14,18	2,4,11,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,7,12,14,16,17	2,4,11,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,7,12,14	2,4,11,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,7,12,14,16,17,18	2,4,11,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,7,12,17,18	2,4,11,13,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,7,12,16	2,4,11,13	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,7,12,17	2,4,11,13,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,7,12,16,18	2,4,11,13,15,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,7,12,14	2,4,11,13	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,7,12,14,16,17,18	2,4,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,7,12,14,18	2,4,11,13,15,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,7,12,14,16,17	2,4,11,13,15,17	$2^{-17.5}$

Table 0.1683 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,7,10,17,18	2,4,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,7,10,16	2,4	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,7,10,17	2,4,15,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,7,10,16,18	2,4,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,7,10,14	2,4	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,7,10,14,16,17,18	2,4,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,7,10,14,18	2,4,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,7,10,14,16,17	2,4,15,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,7,10,17	2,4,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,7,10,16,18	2,4,13,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,7,10,17,18	2,4,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,7,10,16	2,4,13,15	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,7,10,14,18	2,4,13,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,7,10,14,16,17	2,4,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,7,10,14	2,4,13,15	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,7,10,14,16,17,18	2,4,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,7,10,12	2,4	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,7,10,12,16,17,18	2,4,17,18	2^{-34}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,7,10,12,18	2,4,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,7,10,12,16,17	2,4,15,17	2^{-34}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,7,10,12,14,17,18	2,4,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,7,10,12,14,16	2,4	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,7,10,12,14,17	2,4,15,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,7,10,12,14,16,18	2,4,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,7,10,12,18	2,4,13,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,7,10,12,16,17	2,4,13,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,7,10,12	2,4,13,15	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,7,10,12,16,17,18	2,4,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,7,10,12,14,17	2,4,13,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,7,10,12,14,16,18	2,4,13,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,7,10,12,14,17,18	2,4,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,7,10,12,14,16	2,4,13,15	2^{-23}

Table 0.1684 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,7,10,17	2,4,11,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,7,10,16,18	2,4,11,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,7,10,17,18	2,4,11,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,7,10,16	2,4,11,15	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,7,10,14,18	2,4,11,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,7,10,14,16,17	2,4,11,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,7,10,14	2,4,11,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,7,10,14,16,17,18	2,4,11,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,7,10,17,18	2,4,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,7,10,16	2,4,11,13	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,7,10,17	2,4,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,7,10,16,18	2,4,11,13,15,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,7,10,14	2,4,11,13	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,7,10,14,16,17,18	2,4,11,13,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,7,10,14,18	2,4,11,13,15,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,7,10,14,16,17	2,4,11,13,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,7,10,12,18	2,4,11,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,7,10,12,16,17	2,4,11,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,7,10,12	2,4,11,15	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,7,10,12,16,17,18	2,4,11,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,7,10,12,14,17	2,4,11,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,7,10,12,14,16,18	2,4,11,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,7,10,12,14,17,18	2,4,11,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,7,10,12,14,16	2,4,11,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,7,10,12	2,4,11,13	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,7,10,12,16,17,18	2,4,11,13,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,7,10,12,18	2,4,11,13,15,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,7,10,12,16,17	2,4,11,13,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,7,10,12,14,17,18	2,4,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,7,10,12,14,16	2,4,11,13	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,7,10,12,14,17	2,4,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,7,10,12,14,16,18	2,4,11,13,15,18	2^{-12}

Table 0.1685 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,7,18	2,4,9,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,7,16,17	2,4,9,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,7	2,4,9,15	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,7,16,17,18	2,4,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,7,14,17	2,4,9,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,7,14,16,18	2,4,9,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,7,14,17,18	2,4,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,7,14,16	2,4,9,15	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,7	2,4,9,13	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,7,16,17,18	2,4,9,13,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,7,18	2,4,9,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,7,16,17	2,4,9,13,15,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,7,14,17,18	2,4,9,13,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,7,14,16	2,4,9,13	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,7,14,17	2,4,9,13,15,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,7,14,16,18	2,4,9,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,7,12,17	2,4,9,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,7,12,16,18	2,4,9,18	2^{-34}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,7,12,17,18	2,4,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,7,12,16	2,4,9,15	2^{-34}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,7,12,14,18	2,4,9,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,7,12,14,16,17	2,4,9,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,7,12,14	2,4,9,15	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,7,12,14,16,17,18	2,4,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,7,12,17,18	2,4,9,13,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,7,12,16	2,4,9,13	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,7,12,17	2,4,9,13,15,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,7,12,16,18	2,4,9,13,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,7,12,14	2,4,9,13	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,7,12,14,16,17,18	2,4,9,13,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,7,12,14,18	2,4,9,13,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,7,12,14,16,17	2,4,9,13,15,17	2^{-23}

Table 0.1686 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,7	2,4,9,11	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,7,16,17,18	2,4,9,11,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,7,18	2,4,9,11,15,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,7,16,17	2,4,9,11,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,7,14,17,18	2,4,9,11,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,7,14,16	2,4,9,11	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,7,14,17	2,4,9,11,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,7,14,16,18	2,4,9,11,15,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,7,18	2,4,9,11,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,7,16,17	2,4,9,11,13,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,7	2,4,9,11,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,7,16,17,18	2,4,9,11,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,7,14,17	2,4,9,11,13,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,7,14,16,18	2,4,9,11,13,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,7,14,17,18	2,4,9,11,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,7,14,16	2,4,9,11,13,15	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,7,12,17,18	2,4,9,11,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,7,12,16	2,4,9,11	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,7,12,17	2,4,9,11,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,7,12,16,18	2,4,9,11,15,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,7,12,14	2,4,9,11	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,7,12,14,16,17,18	2,4,9,11,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,7,12,14,18	2,4,9,11,15,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,7,12,14,16,17	2,4,9,11,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,7,12,17	2,4,9,11,13,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,7,12,16,18	2,4,9,11,13,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,7,12,17,18	2,4,9,11,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,7,12,16	2,4,9,11,13,15	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,7,12,14,18	2,4,9,11,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,7,12,14,16,17	2,4,9,11,13,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,7,12,14	2,4,9,11,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,7,12,14,16,17,18	2,4,9,11,13,15,17,18	2^{-12}

Table 0.1687 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,7,10,17	2,4,9,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,7,10,16,18	2,4,9,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,7,10,17,18	2,4,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,7,10,16	2,4,9,15	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,7,10,14,18	2,4,9,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,7,10,14,16,17	2,4,9,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,7,10,14	2,4,9,15	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,7,10,14,16,17,18	2,4,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,7,10,17,18	2,4,9,13,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,7,10,16	2,4,9,13	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,7,10,17	2,4,9,13,15,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,7,10,16,18	2,4,9,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,7,10,14	2,4,9,13	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,7,10,14,16,17,18	2,4,9,13,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,7,10,14,18	2,4,9,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,7,10,14,16,17	2,4,9,13,15,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,7,10,12,18	2,4,9,18	2^{-1}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,7,10,12,16,17	2,4,9,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,7,10,12	2,4,9,15	2^{-1}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,7,10,12,16,17,18	2,4,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,7,10,12,14,17	2,4,9,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,7,10,12,14,16,18	2,4,9,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,7,10,12,14,17,18	2,4,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,7,10,12,14,16	2,4,9,15	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,7,10,12	2,4,9,13	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,7,10,12,16,17,18	2,4,9,13,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,7,10,12,18	2,4,9,13,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,7,10,12,16,17	2,4,9,13,15,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,7,10,12,14,17,18	2,4,9,13,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,7,10,12,14,16	2,4,9,13	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,7,10,12,14,17	2,4,9,13,15,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,7,10,12,14,16,18	2,4,9,13,15,18	$2^{-6.5}$

Table 0.1688 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,7,10,17,18	2,4,9,11,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,7,10,16	2,4,9,11	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,7,10,17	2,4,9,11,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,7,10,16,18	2,4,9,11,15,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,7,10,14	2,4,9,11	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,7,10,14,16,17,18	2,4,9,11,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,7,10,14,18	2,4,9,11,15,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,7,10,14,16,17	2,4,9,11,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,7,10,17	2,4,9,11,13,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,7,10,16,18	2,4,9,11,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,7,10,17,18	2,4,9,11,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,7,10,16	2,4,9,11,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,7,10,14,18	2,4,9,11,13,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,7,10,14,16,17	2,4,9,11,13,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,7,10,14	2,4,9,11,13,15	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,7,10,14,16,17,18	2,4,9,11,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,7,10,12	2,4,9,11	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,7,10,12,16,17,18	2,4,9,11,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,7,10,12,18	2,4,9,11,15,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,7,10,12,16,17	2,4,9,11,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,7,10,12,14,17,18	2,4,9,11,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,7,10,12,14,16	2,4,9,11	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,7,10,12,14,17	2,4,9,11,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,7,10,12,14,16,18	2,4,9,11,15,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,7,10,12,18	2,4,9,11,13,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,7,10,12,16,17	2,4,9,11,13,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,7,10,12	2,4,9,11,13,15	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,7,10,12,16,17,18	2,4,9,11,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,7,10,12,14,17	2,4,9,11,13,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,7,10,12,14,16,18	2,4,9,11,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,7,10,12,14,17,18	2,4,9,11,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,7,10,12,14,16	2,4,9,11,13,15	$2^{-17.5}$

Table 0.1689 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,7,17,18	2,4,8,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,7,16	2,4,8	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,7,17	2,4,8,15,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,7,16,18	2,4,8,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,7,14	2,4,8	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,7,14,16,17,18	2,4,8,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,7,14,18	2,4,8,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,7,14,16,17	2,4,8,15,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,7,17	2,4,8,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,7,16,18	2,4,8,13,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,7,17,18	2,4,8,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,7,16	2,4,8,13,15	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,7,14,18	2,4,8,13,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,7,14,16,17	2,4,8,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,7,14	2,4,8,13,15	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,7,14,16,17,18	2,4,8,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,7,12	2,4,8	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,7,12,16,17,18	2,4,8,17,18	2^{-1}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,7,12,18	2,4,8,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,7,12,16,17	2,4,8,15,17	2^{-1}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,7,12,14,17,18	2,4,8,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,7,12,14,16	2,4,8	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,7,12,14,17	2,4,8,15,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,7,12,14,16,18	2,4,8,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,7,12,18	2,4,8,13,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,7,12,16,17	2,4,8,13,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,7,12	2,4,8,13,15	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,7,12,16,17,18	2,4,8,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,7,12,14,17	2,4,8,13,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,7,12,14,16,18	2,4,8,13,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,7,12,14,17,18	2,4,8,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,7,12,14,16	2,4,8,13,15	2^{-12}

Table 0.1690 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,7,17	2,4,8,11,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,7,16,18	2,4,8,11,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,7,17,18	2,4,8,11,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,7,16	2,4,8,11,15	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,7,14,18	2,4,8,11,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,7,14,16,17	2,4,8,11,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,7,14	2,4,8,11,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,7,14,16,17,18	2,4,8,11,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,7,17,18	2,4,8,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,7,16	2,4,8,11,13	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,7,17	2,4,8,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,7,16,18	2,4,8,11,13,15,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,7,14	2,4,8,11,13	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,7,14,16,17,18	2,4,8,11,13,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,7,14,18	2,4,8,11,13,15,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,7,14,16,17	2,4,8,11,13,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,7,12,18	2,4,8,11,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,7,12,16,17	2,4,8,11,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,7,12	2,4,8,11,15	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,7,12,16,17,18	2,4,8,11,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,7,12,14,17	2,4,8,11,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,7,12,14,16,18	2,4,8,11,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,7,12,14,17,18	2,4,8,11,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,7,12,14,16	2,4,8,11,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,7,12	2,4,8,11,13	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,7,12,16,17,18	2,4,8,11,13,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,7,12,18	2,4,8,11,13,15,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,7,12,16,17	2,4,8,11,13,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,7,12,14,17,18	2,4,8,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,7,12,14,16	2,4,8,11,13	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,7,12,14,17	2,4,8,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,7,12,14,16,18	2,4,8,11,13,15,18	2^{-23}

Table 0.1691 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,7,10	2,4,8	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,7,10,16,17,18	2,4,8,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,7,10,18	2,4,8,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,7,10,16,17	2,4,8,15,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,7,10,14,17,18	2,4,8,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,7,10,14,16	2,4,8	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,7,10,14,17	2,4,8,15,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,7,10,14,16,18	2,4,8,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,7,10,18	2,4,8,13,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,7,10,16,17	2,4,8,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,7,10	2,4,8,13,15	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,7,10,16,17,18	2,4,8,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,7,10,14,17	2,4,8,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,7,10,14,16,18	2,4,8,13,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,7,10,14,17,18	2,4,8,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,7,10,14,16	2,4,8,13,15	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,7,10,12,17,18	2,4,8,17,18	2^{-34}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,7,10,12,16	2,4,8	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,7,10,12,17	2,4,8,15,17	2^{-34}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,7,10,12,16,18	2,4,8,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,7,10,12,14	2,4,8	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,7,10,12,14,16,17,18	2,4,8,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,7,10,12,14,18	2,4,8,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,7,10,12,14,16,17	2,4,8,15,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,7,10,12,17	2,4,8,13,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,7,10,12,16,18	2,4,8,13,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,7,10,12,17,18	2,4,8,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,7,10,12,16	2,4,8,13,15	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,7,10,12,14,18	2,4,8,13,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,7,10,12,14,16,17	2,4,8,13,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,7,10,12,14	2,4,8,13,15	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,7,10,12,14,16,17,18	2,4,8,13,15,17,18	$2^{-28.5}$

Table 0.1692 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,7,10,18	2,4,8,11,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,7,10,16,17	2,4,8,11,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,7,10	2,4,8,11,15	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,7,10,16,17,18	2,4,8,11,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,7,10,14,17	2,4,8,11,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,7,10,14,16,18	2,4,8,11,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,7,10,14,17,18	2,4,8,11,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,7,10,14,16	2,4,8,11,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0)$	1,7,10	2,4,8,11,13	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,7,10,16,17,18	2,4,8,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,7,10,18	2,4,8,11,13,15,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,7,10,16,17	2,4,8,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,7,10,14,17,18	2,4,8,11,13,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,7,10,14,16	2,4,8,11,13	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,7,10,14,17	2,4,8,11,13,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,7,10,14,16,18	2,4,8,11,13,15,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,7,10,12,17	2,4,8,11,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,7,10,12,16,18	2,4,8,11,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,7,10,12,17,18	2,4,8,11,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,7,10,12,16	2,4,8,11,15	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,7,10,12,14,18	2,4,8,11,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,7,10,12,14,16,17	2,4,8,11,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,7,10,12,14	2,4,8,11,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,7,10,12,14,16,17,18	2,4,8,11,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,7,10,12,17,18	2,4,8,11,13,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,7,10,12,16	2,4,8,11,13	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,7,10,12,17	2,4,8,11,13,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,7,10,12,16,18	2,4,8,11,13,15,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,7,10,12,14	2,4,8,11,13	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,7,10,12,14,16,17,18	2,4,8,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,7,10,12,14,18	2,4,8,11,13,15,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,7,10,12,14,16,17	2,4,8,11,13,15,17	$2^{-17.5}$

Table 0.1693 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,7,17	2,4,8,9,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,7,16,18	2,4,8,9,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,7,17,18	2,4,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,7,16	2,4,8,9,15	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,7,14,18	2,4,8,9,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,7,14,16,17	2,4,8,9,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,7,14	2,4,8,9,15	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,7,14,16,17,18	2,4,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,7,17,18	2,4,8,9,13,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,7,16	2,4,8,9,13	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,7,17	2,4,8,9,13,15,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,7,16,18	2,4,8,9,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,7,14	2,4,8,9,13	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,7,14,16,17,18	2,4,8,9,13,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,7,14,18	2,4,8,9,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,7,14,16,17	2,4,8,9,13,15,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,7,12,18	2,4,8,9,18	2^{-34}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,7,12,16,17	2,4,8,9,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,7,12	2,4,8,9,15	2^{-34}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,7,12,16,17,18	2,4,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,7,12,14,17	2,4,8,9,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,7,12,14,16,18	2,4,8,9,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,7,12,14,17,18	2,4,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,7,12,14,16	2,4,8,9,15	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,7,12	2,4,8,9,13	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,7,12,16,17,18	2,4,8,9,13,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,7,12,18	2,4,8,9,13,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,7,12,16,17	2,4,8,9,13,15,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,7,12,14,17,18	2,4,8,9,13,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,7,12,14,16	2,4,8,9,13	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,7,12,14,17	2,4,8,9,13,15,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,7,12,14,16,18	2,4,8,9,13,15,18	$2^{-28.5}$

Table 0.1694 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,7,17,18	2,4,8,9,11,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,7,16	2,4,8,9,11	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,7,17	2,4,8,9,11,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,7,16,18	2,4,8,9,11,15,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,7,14	2,4,8,9,11	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,7,14,16,17,18	2,4,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,7,14,18	2,4,8,9,11,15,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,7,14,16,17	2,4,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,7,17	2,4,8,9,11,13,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,7,16,18	2,4,8,9,11,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,7,17,18	2,4,8,9,11,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,7,16	2,4,8,9,11,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,7,14,18	2,4,8,9,11,13,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,7,14,16,17	2,4,8,9,11,13,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,7,14	2,4,8,9,11,13,15	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,7,14,16,17,18	2,4,8,9,11,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,7,12	2,4,8,9,11	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,7,12,16,17,18	2,4,8,9,11,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,7,12,18	2,4,8,9,11,15,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,7,12,16,17	2,4,8,9,11,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,7,12,14,17,18	2,4,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,7,12,14,16	2,4,8,9,11	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,7,12,14,17	2,4,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,7,12,14,16,18	2,4,8,9,11,15,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,7,12,18	2,4,8,9,11,13,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,7,12,16,17	2,4,8,9,11,13,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,7,12	2,4,8,9,11,13,15	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,7,12,16,17,18	2,4,8,9,11,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,7,12,14,17	2,4,8,9,11,13,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,7,12,14,16,18	2,4,8,9,11,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,7,12,14,17,18	2,4,8,9,11,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,7,12,14,16	2,4,8,9,11,13,15	$2^{-17.5}$

Table 0.1695 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,7,10,18	2,4,8,9,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,7,10,16,17	2,4,8,9,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,7,10	2,4,8,9,15	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,7,10,16,17,18	2,4,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,7,10,14,17	2,4,8,9,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,7,10,14,16,18	2,4,8,9,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,7,10,14,17,18	2,4,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,7,10,14,16	2,4,8,9,15	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,7,10	2,4,8,9,13	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,7,10,16,17,18	2,4,8,9,13,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,7,10,18	2,4,8,9,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,7,10,16,17	2,4,8,9,13,15,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,7,10,14,17,18	2,4,8,9,13,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,7,10,14,16	2,4,8,9,13	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,7,10,14,17	2,4,8,9,13,15,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,7,10,14,16,18	2,4,8,9,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,7,10,12,17	2,4,8,9,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,7,10,12,16,18	2,4,8,9,18	2^{-1}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,7,10,12,17,18	2,4,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,7,10,12,16	2,4,8,9,15	2^{-1}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,7,10,12,14,18	2,4,8,9,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,7,10,12,14,16,17	2,4,8,9,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,7,10,12,14	2,4,8,9,15	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,7,10,12,14,16,17,18	2,4,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,7,10,12,17,18	2,4,8,9,13,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,7,10,12,16	2,4,8,9,13	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,7,10,12,17	2,4,8,9,13,15,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,7,10,12,16,18	2,4,8,9,13,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,7,10,12,14	2,4,8,9,13	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,7,10,12,14,16,17,18	2,4,8,9,13,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,7,10,12,14,18	2,4,8,9,13,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,7,10,12,14,16,17	2,4,8,9,13,15,17	2^{-12}

Table 0.1696 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,7,10	2,4,8,9,11	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,7,10,16,17,18	2,4,8,9,11,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,7,10,18	2,4,8,9,11,15,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,7,10,16,17	2,4,8,9,11,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,7,10,14,17,18	2,4,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,7,10,14,16	2,4,8,9,11	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,7,10,14,17	2,4,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,7,10,14,16,18	2,4,8,9,11,15,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,7,10,18	2,4,8,9,11,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,7,10,16,17	2,4,8,9,11,13,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,7,10	2,4,8,9,11,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,7,10,16,17,18	2,4,8,9,11,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,7,10,14,17	2,4,8,9,11,13,17	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,7,10,14,16,18	2,4,8,9,11,13,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,7,10,14,17,18	2,4,8,9,11,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,7,10,14,16	2,4,8,9,11,13,15	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,7,10,12,17,18	2,4,8,9,11,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,7,10,12,16	2,4,8,9,11	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,7,10,12,17	2,4,8,9,11,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,7,10,12,16,18	2,4,8,9,11,15,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,7,10,12,14	2,4,8,9,11	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,7,10,12,14,16,17,18	2,4,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,7,10,12,14,18	2,4,8,9,11,15,18	2^{-12}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,7,10,12,14,16,17	2,4,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,7,10,12,17	2,4,8,9,11,13,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,7,10,12,16,18	2,4,8,9,11,13,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,7,10,12,17,18	2,4,8,9,11,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,7,10,12,16	2,4,8,9,11,13,15	$2^{-6.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,7,10,12,14,18	2,4,8,9,11,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,7,10,12,14,16,17	2,4,8,9,11,13,17	2^{-23}
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,7,10,12,14	2,4,8,9,11,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,7,10,12,14,16,17,18	2,4,8,9,11,13,15,17,18	2^{-23}

Table 0.1697 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,17	2,4,6,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,16,18	2,4,6,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,17,18	2,4,6,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,16	2,4,6,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,14,18	2,4,6,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,14,16,17	2,4,6,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,14	2,4,6,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,14,16,17,18	2,4,6,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,17,18	2,4,6,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,16	2,4,6,13	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,17	2,4,6,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,16,18	2,4,6,13,15,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,14	2,4,6,13	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,14,16,17,18	2,4,6,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,14,18	2,4,6,13,15,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,14,16,17	2,4,6,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,12,18	2,4,6,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,12,16,17	2,4,6,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,12	2,4,6,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,12,16,17,18	2,4,6,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,12,14,17	2,4,6,17	2^{-1}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,12,14,16,18	2,4,6,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,12,14,17,18	2,4,6,15,17,18	2^{-1}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,12,14,16	2,4,6,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,12	2,4,6,13	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,12,16,17,18	2,4,6,13,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,12,18	2,4,6,13,15,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,12,16,17	2,4,6,13,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,12,14,17,18	2,4,6,13,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,12,14,16	2,4,6,13	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,12,14,17	2,4,6,13,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,12,14,16,18	2,4,6,13,15,18	2^{-23}

Table 0.1698 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,17,18	2,4,6,11,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,16	2,4,6,11	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,17	2,4,6,11,15,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,16,18	2,4,6,11,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,14	2,4,6,11	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,14,16,17,18	2,4,6,11,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,14,18	2,4,6,11,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,14,16,17	2,4,6,11,15,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,17	2,4,6,11,13,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,16,18	2,4,6,11,13,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,17,18	2,4,6,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,16	2,4,6,11,13,15	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,14,18	2,4,6,11,13,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,14,16,17	2,4,6,11,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,14	2,4,6,11,13,15	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,14,16,17,18	2,4,6,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,12	2,4,6,11	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,12,16,17,18	2,4,6,11,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,12,18	2,4,6,11,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,12,16,17	2,4,6,11,15,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,12,14,17,18	2,4,6,11,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,12,14,16	2,4,6,11	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,12,14,17	2,4,6,11,15,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,12,14,16,18	2,4,6,11,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,12,18	2,4,6,11,13,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,12,16,17	2,4,6,11,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,12	2,4,6,11,13,15	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,12,16,17,18	2,4,6,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,12,14,17	2,4,6,11,13,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,12,14,16,18	2,4,6,11,13,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,12,14,17,18	2,4,6,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,12,14,16	2,4,6,11,13,15	2^{-23}

Table 0.1699 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,10,18	2,4,6,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,10,16,17	2,4,6,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,10	2,4,6,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,10,16,17,18	2,4,6,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,10,14,17	2,4,6,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,10,14,16,18	2,4,6,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,10,14,17,18	2,4,6,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,10,14,16	2,4,6,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,10	2,4,6,13	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,10,16,17,18	2,4,6,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,10,18	2,4,6,13,15,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,10,16,17	2,4,6,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,10,14,17,18	2,4,6,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,10,14,16	2,4,6,13	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,10,14,17	2,4,6,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,10,14,16,18	2,4,6,13,15,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,10,12,17	2,4,6,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,10,12,16,18	2,4,6,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,10,12,17,18	2,4,6,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,10,12,16	2,4,6,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,10,12,14,18	2,4,6,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,10,12,14,16,17	2,4,6,17	2^{-34}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,10,12,14	2,4,6,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,10,12,14,16,17,18	2,4,6,15,17,18	2^{-34}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,10,12,17,18	2,4,6,13,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,10,12,16	2,4,6,13	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,10,12,17	2,4,6,13,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,10,12,16,18	2,4,6,13,15,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,10,12,14	2,4,6,13	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,10,12,14,16,17,18	2,4,6,13,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,10,12,14,18	2,4,6,13,15,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,10,12,14,16,17	2,4,6,13,15,17	$2^{-28.5}$

Table 0.1700 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,10	2,4,6,11	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,10,16,17,18	2,4,6,11,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,10,18	2,4,6,11,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,10,16,17	2,4,6,11,15,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,10,14,17,18	2,4,6,11,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,10,14,16	2,4,6,11	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,10,14,17	2,4,6,11,15,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,10,14,16,18	2,4,6,11,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,10,18	2,4,6,11,13,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,10,16,17	2,4,6,11,13,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,10	2,4,6,11,13,15	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,10,16,17,18	2,4,6,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,10,14,17	2,4,6,11,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,10,14,16,18	2,4,6,11,13,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,10,14,17,18	2,4,6,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,10,14,16	2,4,6,11,13,15	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,10,12,17,18	2,4,6,11,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,10,12,16	2,4,6,11	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,10,12,17	2,4,6,11,15,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,10,12,16,18	2,4,6,11,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,10,12,14	2,4,6,11	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,10,12,14,16,17,18	2,4,6,11,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,10,12,14,18	2,4,6,11,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,10,12,14,16,17	2,4,6,11,15,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,10,12,17	2,4,6,11,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,10,12,16,18	2,4,6,11,13,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,10,12,17,18	2,4,6,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,10,12,16	2,4,6,11,13,15	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,10,12,14,18	2,4,6,11,13,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,10,12,14,16,17	2,4,6,11,13,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,10,12,14	2,4,6,11,13,15	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,10,12,14,16,17,18	2,4,6,11,13,15,17,18	$2^{-28.5}$

Table 0.1701 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,17,18	2,4,6,9,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,16	2,4,6,9	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,17	2,4,6,9,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,16,18	2,4,6,9,15,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,14	2,4,6,9	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,14,16,17,18	2,4,6,9,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,14,18	2,4,6,9,15,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,14,16,17	2,4,6,9,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,17	2,4,6,9,13,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,16,18	2,4,6,9,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,17,18	2,4,6,9,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,16	2,4,6,9,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,14,18	2,4,6,9,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,14,16,17	2,4,6,9,13,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,14	2,4,6,9,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,14,16,17,18	2,4,6,9,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,12	2,4,6,9	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,12,16,17,18	2,4,6,9,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,12,18	2,4,6,9,15,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,12,16,17	2,4,6,9,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,12,14,17,18	2,4,6,9,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,12,14,16	2,4,6,9	2^{-34}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,12,14,17	2,4,6,9,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,12,14,16,18	2,4,6,9,15,18	2^{-34}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,12,18	2,4,6,9,13,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,12,16,17	2,4,6,9,13,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,12	2,4,6,9,13,15	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,12,16,17,18	2,4,6,9,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,12,14,17	2,4,6,9,13,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,12,14,16,18	2,4,6,9,13,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,12,14,17,18	2,4,6,9,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,12,14,16	2,4,6,9,13,15	$2^{-28.5}$

Table 0.1702 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,17	2,4,6,9,11,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,16,18	2,4,6,9,11,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,17,18	2,4,6,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,16	2,4,6,9,11,15	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,14,18	2,4,6,9,11,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0)$	1,14,16,17	2,4,6,9,11,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,14	2,4,6,9,11,15	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,14,16,17,18	2,4,6,9,11,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,17,18	2,4,6,9,11,13,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,16	2,4,6,9,11,13	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,17	2,4,6,9,11,13,15,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,16,18	2,4,6,9,11,13,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,14	2,4,6,9,11,13	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,14,16,17,18	2,4,6,9,11,13,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,14,18	2,4,6,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,14,16,17	2,4,6,9,11,13,15,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,12,18	2,4,6,9,11,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,12,16,17	2,4,6,9,11,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,12	2,4,6,9,11,15	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,12,16,17,18	2,4,6,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,12,14,17	2,4,6,9,11,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,12,14,16,18	2,4,6,9,11,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,12,14,17,18	2,4,6,9,11,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,12,14,16	2,4,6,9,11,15	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,12	2,4,6,9,11,13	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,12,16,17,18	2,4,6,9,11,13,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,12,18	2,4,6,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,12,16,17	2,4,6,9,11,13,15,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,12,14,17,18	2,4,6,9,11,13,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,12,14,16	2,4,6,9,11,13	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,12,14,17	2,4,6,9,11,13,15,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,12,14,16,18	2,4,6,9,11,13,15,18	$2^{-28.5}$

Table 0.1703 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,10	2,4,6,9	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,10,16,17,18	2,4,6,9,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,10,18	2,4,6,9,15,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,10,16,17	2,4,6,9,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,10,14,17,18	2,4,6,9,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,10,14,16	2,4,6,9	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,10,14,17	2,4,6,9,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,10,14,16,18	2,4,6,9,15,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,10,18	2,4,6,9,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,10,16,17	2,4,6,9,13,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,10	2,4,6,9,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,10,16,17,18	2,4,6,9,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,10,14,17	2,4,6,9,13,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,10,14,16,18	2,4,6,9,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,10,14,17,18	2,4,6,9,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,10,14,16	2,4,6,9,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,10,12,17,18	2,4,6,9,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,10,12,16	2,4,6,9	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,10,12,17	2,4,6,9,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,10,12,16,18	2,4,6,9,15,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,10,12,14	2,4,6,9	2^{-1}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,10,12,14,16,17,18	2,4,6,9,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,10,12,14,18	2,4,6,9,15,18	2^{-1}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,10,12,14,16,17	2,4,6,9,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,10,12,17	2,4,6,9,13,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,10,12,16,18	2,4,6,9,13,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,10,12,17,18	2,4,6,9,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,10,12,16	2,4,6,9,13,15	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,10,12,14,18	2,4,6,9,13,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,10,12,14,16,17	2,4,6,9,13,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,10,12,14	2,4,6,9,13,15	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,10,12,14,16,17,18	2,4,6,9,13,15,17,18	2^{-23}

Table 0.1704 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,10,18	2,4,6,9,11,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,10,16,17	2,4,6,9,11,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,10	2,4,6,9,11,15	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,10,16,17,18	2,4,6,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,10,14,17	2,4,6,9,11,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,10,14,16,18	2,4,6,9,11,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,10,14,17,18	2,4,6,9,11,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,10,14,16	2,4,6,9,11,15	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,10	2,4,6,9,11,13	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,10,16,17,18	2,4,6,9,11,13,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,10,18	2,4,6,9,11,13,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,10,16,17	2,4,6,9,11,13,15,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,10,14,17,18	2,4,6,9,11,13,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,10,14,16	2,4,6,9,11,13	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,10,14,17	2,4,6,9,11,13,15,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,10,14,16,18	2,4,6,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,10,12,17	2,4,6,9,11,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,10,12,16,18	2,4,6,9,11,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,10,12,17,18	2,4,6,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,10,12,16	2,4,6,9,11,15	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,10,12,14,18	2,4,6,9,11,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,10,12,14,16,17	2,4,6,9,11,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,10,12,14	2,4,6,9,11,15	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,10,12,14,16,17,18	2,4,6,9,11,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,10,12,17,18	2,4,6,9,11,13,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,10,12,16	2,4,6,9,11,13	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,10,12,17	2,4,6,9,11,13,15,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,10,12,16,18	2,4,6,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,10,12,14	2,4,6,9,11,13	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,10,12,14,16,17,18	2,4,6,9,11,13,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,10,12,14,18	2,4,6,9,11,13,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,10,12,14,16,17	2,4,6,9,11,13,15,17	2^{-23}

Table 0.1705 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,18	2,4,6,8,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,16,17	2,4,6,8,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1	2,4,6,8,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,16,17,18	2,4,6,8,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,14,17	2,4,6,8,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,14,16,18	2,4,6,8,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,14,17,18	2,4,6,8,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,14,16	2,4,6,8,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1	2,4,6,8,13	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,16,17,18	2,4,6,8,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,18	2,4,6,8,13,15,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,16,17	2,4,6,8,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,14,17,18	2,4,6,8,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,14,16	2,4,6,8,13	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,14,17	2,4,6,8,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,14,16,18	2,4,6,8,13,15,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,12,17	2,4,6,8,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,12,16,18	2,4,6,8,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,12,17,18	2,4,6,8,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,12,16	2,4,6,8,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,12,14,18	2,4,6,8,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,12,14,16,17	2,4,6,8,17	2^{-1}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,12,14	2,4,6,8,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,12,14,16,17,18	2,4,6,8,15,17,18	2^{-1}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,12,17,18	2,4,6,8,13,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,12,16	2,4,6,8,13	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,12,17	2,4,6,8,13,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,12,16,18	2,4,6,8,13,15,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,12,14	2,4,6,8,13	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,12,14,16,17,18	2,4,6,8,13,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,12,14,18	2,4,6,8,13,15,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,12,14,16,17	2,4,6,8,13,15,17	$2^{-6.5}$

Table 0.1706 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1	2,4,6,8,11	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,16,17,18	2,4,6,8,11,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,18	2,4,6,8,11,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,16,17	2,4,6,8,11,15,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,14,17,18	2,4,6,8,11,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,14,16	2,4,6,8,11	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,14,17	2,4,6,8,11,15,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,14,16,18	2,4,6,8,11,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,18	2,4,6,8,11,13,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,16,17	2,4,6,8,11,13,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1	2,4,6,8,11,13,15	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,16,17,18	2,4,6,8,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,14,17	2,4,6,8,11,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,14,16,18	2,4,6,8,11,13,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,14,17,18	2,4,6,8,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,14,16	2,4,6,8,11,13,15	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,12,17,18	2,4,6,8,11,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,12,16	2,4,6,8,11	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,12,17	2,4,6,8,11,15,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,12,16,18	2,4,6,8,11,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,12,14	2,4,6,8,11	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,12,14,16,17,18	2,4,6,8,11,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,12,14,18	2,4,6,8,11,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,12,14,16,17	2,4,6,8,11,15,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,12,17	2,4,6,8,11,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,12,16,18	2,4,6,8,11,13,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,12,17,18	2,4,6,8,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,12,16	2,4,6,8,11,13,15	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,12,14,18	2,4,6,8,11,13,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,12,14,16,17	2,4,6,8,11,13,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,12,14	2,4,6,8,11,13,15	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,12,14,16,17,18	2,4,6,8,11,13,15,17,18	$2^{-6.5}$

Table 0.1707 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,10,17	2,4,6,8,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,10,16,18	2,4,6,8,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,10,17,18	2,4,6,8,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,10,16	2,4,6,8,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,10,14,18	2,4,6,8,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,10,14,16,17	2,4,6,8,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,10,14	2,4,6,8,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,10,14,16,17,18	2,4,6,8,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,10,17,18	2,4,6,8,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,10,16	2,4,6,8,13	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,10,17	2,4,6,8,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,10,16,18	2,4,6,8,13,15,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,10,14	2,4,6,8,13	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,10,14,16,17,18	2,4,6,8,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,10,14,18	2,4,6,8,13,15,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,10,14,16,17	2,4,6,8,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,10,12,18	2,4,6,8,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,10,12,16,17	2,4,6,8,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,10,12	2,4,6,8,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,10,12,16,17,18	2,4,6,8,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,10,12,14,17	2,4,6,8,17	2^{-34}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,10,12,14,16,18	2,4,6,8,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,10,12,14,17,18	2,4,6,8,15,17,18	2^{-34}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,10,12,14,16	2,4,6,8,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,10,12	2,4,6,8,13	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,10,12,16,17,18	2,4,6,8,13,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,10,12,18	2,4,6,8,13,15,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,10,12,16,17	2,4,6,8,13,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,10,12,14,17,18	2,4,6,8,13,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,10,12,14,16	2,4,6,8,13	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,10,12,14,17	2,4,6,8,13,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,10,12,14,16,18	2,4,6,8,13,15,18	2^{-12}

Table 0.1708 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,10,17,18	2,4,6,8,11,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,10,16	2,4,6,8,11	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,10,17	2,4,6,8,11,15,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,10,16,18	2,4,6,8,11,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,10,14	2,4,6,8,11	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,10,14,16,17,18	2,4,6,8,11,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,10,14,18	2,4,6,8,11,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,10,14,16,17	2,4,6,8,11,15,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,10,17	2,4,6,8,11,13,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,10,16,18	2,4,6,8,11,13,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,10,17,18	2,4,6,8,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,10,16	2,4,6,8,11,13,15	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,10,14,18	2,4,6,8,11,13,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,10,14,16,17	2,4,6,8,11,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,10,14	2,4,6,8,11,13,15	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,10,14,16,17,18	2,4,6,8,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,10,12	2,4,6,8,11	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,10,12,16,17,18	2,4,6,8,11,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,10,12,18	2,4,6,8,11,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,10,12,16,17	2,4,6,8,11,15,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,10,12,14,17,18	2,4,6,8,11,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,10,12,14,16	2,4,6,8,11	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,10,12,14,17	2,4,6,8,11,15,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,10,12,14,16,18	2,4,6,8,11,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,10,12,18	2,4,6,8,11,13,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,10,12,16,17	2,4,6,8,11,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,10,12	2,4,6,8,11,13,15	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,10,12,16,17,18	2,4,6,8,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,10,12,14,17	2,4,6,8,11,13,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,10,12,14,16,18	2,4,6,8,11,13,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,10,12,14,17,18	2,4,6,8,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,10,12,14,16	2,4,6,8,11,13,15	2^{-12}

Table 0.1709 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1	2,4,6,8,9	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,16,17,18	2,4,6,8,9,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,18	2,4,6,8,9,15,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,16,17	2,4,6,8,9,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1)$	1,14,17,18	2,4,6,8,9,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,14,16	2,4,6,8,9	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,14,17	2,4,6,8,9,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,14,16,18	2,4,6,8,9,15,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,18	2,4,6,8,9,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,16,17	2,4,6,8,9,13,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1	2,4,6,8,9,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,16,17,18	2,4,6,8,9,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,14,17	2,4,6,8,9,13,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,14,16,18	2,4,6,8,9,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,14,17,18	2,4,6,8,9,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,14,16	2,4,6,8,9,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,12,17,18	2,4,6,8,9,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,12,16	2,4,6,8,9	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,12,17	2,4,6,8,9,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,12,16,18	2,4,6,8,9,15,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,12,14	2,4,6,8,9	2^{-34}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,12,14,16,17,18	2,4,6,8,9,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,12,14,18	2,4,6,8,9,15,18	2^{-34}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,12,14,16,17	2,4,6,8,9,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,12,17	2,4,6,8,9,13,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,12,16,18	2,4,6,8,9,13,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,12,17,18	2,4,6,8,9,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,12,16	2,4,6,8,9,13,15	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,12,14,18	2,4,6,8,9,13,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,12,14,16,17	2,4,6,8,9,13,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,12,14	2,4,6,8,9,13,15	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,12,14,16,17,18	2,4,6,8,9,13,15,17,18	2^{-12}

Table 0.1710 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,18	2,4,6,8,9,11,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,16,17	2,4,6,8,9,11,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1	2,4,6,8,9,11,15	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,16,17,18	2,4,6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,14,17	2,4,6,8,9,11,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,14,16,18	2,4,6,8,9,11,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,14,17,18	2,4,6,8,9,11,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,14,16	2,4,6,8,9,11,15	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1	2,4,6,8,9,11,13	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,16,17,18	2,4,6,8,9,11,13,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,18	2,4,6,8,9,11,13,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,16,17	2,4,6,8,9,11,13,15,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,14,17,18	2,4,6,8,9,11,13,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,14,16	2,4,6,8,9,11,13	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,14,17	2,4,6,8,9,11,13,15,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,14,16,18	2,4,6,8,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,12,17	2,4,6,8,9,11,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,12,16,18	2,4,6,8,9,11,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,12,17,18	2,4,6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,12,16	2,4,6,8,9,11,15	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,12,14,18	2,4,6,8,9,11,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,12,14,16,17	2,4,6,8,9,11,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,12,14	2,4,6,8,9,11,15	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,12,14,16,17,18	2,4,6,8,9,11,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,12,17,18	2,4,6,8,9,11,13,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,12,16	2,4,6,8,9,11,13	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,12,17	2,4,6,8,9,11,13,15,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,12,16,18	2,4,6,8,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,12,14	2,4,6,8,9,11,13	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,12,14,16,17,18	2,4,6,8,9,11,13,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,12,14,18	2,4,6,8,9,11,13,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,12,14,16,17	2,4,6,8,9,11,13,15,17	2^{-12}

Table 0.1711 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,10,17,18	2,4,6,8,9,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,10,16	2,4,6,8,9	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,10,17	2,4,6,8,9,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,10,16,18	2,4,6,8,9,15,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,10,14	2,4,6,8,9	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,10,14,16,17,18	2,4,6,8,9,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,10,14,18	2,4,6,8,9,15,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,10,14,16,17	2,4,6,8,9,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,10,17	2,4,6,8,9,13,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,10,16,18	2,4,6,8,9,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,10,17,18	2,4,6,8,9,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,10,16	2,4,6,8,9,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,10,14,18	2,4,6,8,9,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,10,14,16,17	2,4,6,8,9,13,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,10,14	2,4,6,8,9,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,10,14,16,17,18	2,4,6,8,9,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,10,12	2,4,6,8,9	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,10,12,16,17,18	2,4,6,8,9,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,10,12,18	2,4,6,8,9,15,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,10,12,16,17	2,4,6,8,9,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,10,12,14,17,18	2,4,6,8,9,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,10,12,14,16	2,4,6,8,9	2^{-1}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,10,12,14,17	2,4,6,8,9,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,10,12,14,16,18	2,4,6,8,9,15,18	2^{-1}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,10,12,18	2,4,6,8,9,13,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,10,12,16,17	2,4,6,8,9,13,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,10,12	2,4,6,8,9,13,15	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,10,12,16,17,18	2,4,6,8,9,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,10,12,14,17	2,4,6,8,9,13,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,10,12,14,16,18	2,4,6,8,9,13,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,10,12,14,17,18	2,4,6,8,9,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,10,12,14,16	2,4,6,8,9,13,15	$2^{-6.5}$

Table 0.1712 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,10,17	2,4,6,8,9,11,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,10,16,18	2,4,6,8,9,11,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,10,17,18	2,4,6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,10,16	2,4,6,8,9,11,15	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,10,14,18	2,4,6,8,9,11,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,10,14,16,17	2,4,6,8,9,11,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,10,14	2,4,6,8,9,11,15	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,10,14,16,17,18	2,4,6,8,9,11,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,10,17,18	2,4,6,8,9,11,13,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,10,16	2,4,6,8,9,11,13	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,10,17	2,4,6,8,9,11,13,15,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,10,16,18	2,4,6,8,9,11,13,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,10,14	2,4,6,8,9,11,13	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,10,14,16,17,18	2,4,6,8,9,11,13,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,10,14,18	2,4,6,8,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,10,14,16,17	2,4,6,8,9,11,13,15,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,10,12,18	2,4,6,8,9,11,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,10,12,16,17	2,4,6,8,9,11,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,10,12	2,4,6,8,9,11,15	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,10,12,16,17,18	2,4,6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,10,12,14,17	2,4,6,8,9,11,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,10,12,14,16,18	2,4,6,8,9,11,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,10,12,14,17,18	2,4,6,8,9,11,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,10,12,14,16	2,4,6,8,9,11,15	2^{-12}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,10,12	2,4,6,8,9,11,13	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,10,12,16,17,18	2,4,6,8,9,11,13,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,10,12,18	2,4,6,8,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,10,12,16,17	2,4,6,8,9,11,13,15,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,10,12,14,17,18	2,4,6,8,9,11,13,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,10,12,14,16	2,4,6,8,9,11,13	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,10,12,14,17	2,4,6,8,9,11,13,15,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,10,12,14,16,18	2,4,6,8,9,11,13,15,18	$2^{-6.5}$

Table 0.1713 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,7,17,18	2,4,6,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,7,16	2,4,6	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,7,17	2,4,6,15,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,7,16,18	2,4,6,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,7,14	2,4,6	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,7,14,16,17,18	2,4,6,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,7,14,18	2,4,6,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,7,14,16,17	2,4,6,15,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,7,17	2,4,6,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,7,16,18	2,4,6,13,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,7,17,18	2,4,6,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,7,16	2,4,6,13,15	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,7,14,18	2,4,6,13,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,7,14,16,17	2,4,6,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,7,14	2,4,6,13,15	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,7,14,16,17,18	2,4,6,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,7,12	2,4,6	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,7,12,16,17,18	2,4,6,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,7,12,18	2,4,6,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,7,12,16,17	2,4,6,15,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,7,12,14,17,18	2,4,6,17,18	2^{-1}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,7,12,14,16	2,4,6	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,7,12,14,17	2,4,6,15,17	2^{-1}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,7,12,14,16,18	2,4,6,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,7,12,18	2,4,6,13,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,7,12,16,17	2,4,6,13,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,7,12	2,4,6,13,15	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,7,12,16,17,18	2,4,6,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,7,12,14,17	2,4,6,13,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,7,12,14,16,18	2,4,6,13,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,7,12,14,17,18	2,4,6,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,7,12,14,16	2,4,6,13,15	2^{-23}

Table 0.1714 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,7,17	2,4,6,11,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,7,16,18	2,4,6,11,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,7,17,18	2,4,6,11,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,7,16	2,4,6,11,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,7,14,18	2,4,6,11,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,7,14,16,17	2,4,6,11,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,7,14	2,4,6,11,15	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,7,14,16,17,18	2,4,6,11,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,7,17,18	2,4,6,11,13,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,7,16	2,4,6,11,13	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,7,17	2,4,6,11,13,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,7,16,18	2,4,6,11,13,15,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,7,14	2,4,6,11,13	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,7,14,16,17,18	2,4,6,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,7,14,18	2,4,6,11,13,15,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,7,14,16,17	2,4,6,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,7,12,18	2,4,6,11,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,7,12,16,17	2,4,6,11,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,7,12	2,4,6,11,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,7,12,16,17,18	2,4,6,11,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,7,12,14,17	2,4,6,11,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,7,12,14,16,18	2,4,6,11,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,7,12,14,17,18	2,4,6,11,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,7,12,14,16	2,4,6,11,15	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,7,12	2,4,6,11,13	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,7,12,16,17,18	2,4,6,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,7,12,18	2,4,6,11,13,15,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,7,12,16,17	2,4,6,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,7,12,14,17,18	2,4,6,11,13,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,7,12,14,16	2,4,6,11,13	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,7,12,14,17	2,4,6,11,13,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,7,12,14,16,18	2,4,6,11,13,15,18	2^{-23}

Table 0.1715 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,7,10	2,4,6	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,7,10,16,17,18	2,4,6,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,7,10,18	2,4,6,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,7,10,16,17	2,4,6,15,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,7,10,14,17,18	2,4,6,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,7,10,14,16	2,4,6	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,7,10,14,17	2,4,6,15,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,7,10,14,16,18	2,4,6,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,7,10,18	2,4,6,13,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,7,10,16,17	2,4,6,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,7,10	2,4,6,13,15	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,7,10,16,17,18	2,4,6,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,7,10,14,17	2,4,6,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,7,10,14,16,18	2,4,6,13,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,7,10,14,17,18	2,4,6,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,7,10,14,16	2,4,6,13,15	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,7,10,12,17,18	2,4,6,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,7,10,12,16	2,4,6	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,7,10,12,17	2,4,6,15,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,7,10,12,16,18	2,4,6,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,7,10,12,14	2,4,6	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,7,10,12,14,16,17,18	2,4,6,17,18	2^{-34}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,7,10,12,14,18	2,4,6,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,7,10,12,14,16,17	2,4,6,15,17	2^{-34}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,7,10,12,17	2,4,6,13,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,7,10,12,16,18	2,4,6,13,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,7,10,12,17,18	2,4,6,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,7,10,12,16	2,4,6,13,15	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,7,10,12,14,18	2,4,6,13,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,7,10,12,14,16,17	2,4,6,13,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,7,10,12,14	2,4,6,13,15	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,7,10,12,14,16,17,18	2,4,6,13,15,17,18	$2^{-28.5}$

Table 0.1716 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,7,10,18	2,4,6,11,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,7,10,16,17	2,4,6,11,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,7,10	2,4,6,11,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,7,10,16,17,18	2,4,6,11,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,7,10,14,17	2,4,6,11,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,7,10,14,16,18	2,4,6,11,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,7,10,14,17,18	2,4,6,11,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,7,10,14,16	2,4,6,11,15	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,7,10	2,4,6,11,13	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,7,10,16,17,18	2,4,6,11,13,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,7,10,18	2,4,6,11,13,15,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,7,10,16,17	2,4,6,11,13,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,7,10,14,17,18	2,4,6,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,7,10,14,16	2,4,6,11,13	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,7,10,14,17	2,4,6,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,7,10,14,16,18	2,4,6,11,13,15,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,7,10,12,17	2,4,6,11,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,7,10,12,16,18	2,4,6,11,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,7,10,12,17,18	2,4,6,11,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,7,10,12,16	2,4,6,11,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,7,10,12,14,18	2,4,6,11,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,7,10,12,14,16,17	2,4,6,11,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,7,10,12,14	2,4,6,11,15	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,7,10,12,14,16,17,18	2,4,6,11,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,7,10,12,17,18	2,4,6,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,7,10,12,16	2,4,6,11,13	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,7,10,12,17	2,4,6,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,7,10,12,16,18	2,4,6,11,13,15,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,7,10,12,14	2,4,6,11,13	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,7,10,12,14,16,17,18	2,4,6,11,13,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,7,10,12,14,18	2,4,6,11,13,15,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,7,10,12,14,16,17	2,4,6,11,13,15,17	$2^{-28.5}$

Table 0.1717 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,7,17	2,4,6,9,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,7,16,18	2,4,6,9,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,7,17,18	2,4,6,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,7,16	2,4,6,9,15	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,7,14,18	2,4,6,9,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,7,14,16,17	2,4,6,9,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,7,14	2,4,6,9,15	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,7,14,16,17,18	2,4,6,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,7,17,18	2,4,6,9,13,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,7,16	2,4,6,9,13	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,7,17	2,4,6,9,13,15,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,7,16,18	2,4,6,9,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,7,14	2,4,6,9,13	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,7,14,16,17,18	2,4,6,9,13,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,7,14,18	2,4,6,9,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,7,14,16,17	2,4,6,9,13,15,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,7,12,18	2,4,6,9,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,7,12,16,17	2,4,6,9,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,7,12	2,4,6,9,15	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,7,12,16,17,18	2,4,6,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,7,12,14,17	2,4,6,9,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,7,12,14,16,18	2,4,6,9,18	2^{-34}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1)$	1,7,12,14,17,18	2,4,6,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,7,12,14,16	2,4,6,9,15	2^{-34}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,7,12	2,4,6,9,13	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,7,12,16,17,18	2,4,6,9,13,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,7,12,18	2,4,6,9,13,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,7,12,16,17	2,4,6,9,13,15,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,7,12,14,17,18	2,4,6,9,13,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,7,12,14,16	2,4,6,9,13	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,7,12,14,17	2,4,6,9,13,15,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,7,12,14,16,18	2,4,6,9,13,15,18	$2^{-28.5}$

Table 0.1718 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,7,17,18	2,4,6,9,11,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,7,16	2,4,6,9,11	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,7,17	2,4,6,9,11,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,7,16,18	2,4,6,9,11,15,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,7,14	2,4,6,9,11	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,7,14,16,17,18	2,4,6,9,11,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,7,14,18	2,4,6,9,11,15,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,7,14,16,17	2,4,6,9,11,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,7,17	2,4,6,9,11,13,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,7,16,18	2,4,6,9,11,13,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,7,17,18	2,4,6,9,11,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,7,16	2,4,6,9,11,13,15	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,7,14,18	2,4,6,9,11,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,7,14,16,17	2,4,6,9,11,13,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,7,16,18	2,4,6,9,11,13,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,7,17,18	2,4,6,9,11,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,7,16	2,4,6,9,11,13,15	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,7,14,18	2,4,6,9,11,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,7,14,16,17	2,4,6,9,11,13,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,7,14	2,4,6,9,11,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,7,14,16,17,18	2,4,6,9,11,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,7,12	2,4,6,9,11	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,7,12,16,17,18	2,4,6,9,11,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,7,12,18	2,4,6,9,11,15,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,7,12,16,17	2,4,6,9,11,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,7,12,14,17,18	2,4,6,9,11,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,7,12,14,16	2,4,6,9,11	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,7,12,14,17	2,4,6,9,11,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,7,12,14,16,18	2,4,6,9,11,15,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,7,12,18	2,4,6,9,11,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,7,12,16,17	2,4,6,9,11,13,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,7,12	2,4,6,9,11,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,7,12,16,17,18	2,4,6,9,11,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,7,12,14,17	2,4,6,9,11,13,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,7,12,14,16,18	2,4,6,9,11,13,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,7,12,14,17,18	2,4,6,9,11,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,7,12,14,16	2,4,6,9,11,13,15	$2^{-28.5}$

Table 0.1719 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,7,10,18	2,4,6,9,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,7,10,16,17	2,4,6,9,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,7,10	2,4,6,9,15	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,7,10,16,17,18	2,4,6,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,7,10,14,17	2,4,6,9,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,7,10,14,16,18	2,4,6,9,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,7,10,14,17,18	2,4,6,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,7,10,14,16	2,4,6,9,15	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,7,10	2,4,6,9,13	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,7,10,16,17,18	2,4,6,9,13,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,7,10,18	2,4,6,9,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,7,10,16,17	2,4,6,9,13,15,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,7,10,14,17,18	2,4,6,9,13,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,7,10,14,16	2,4,6,9,13	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,7,10,14,17	2,4,6,9,13,15,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,7,10,14,16,18	2,4,6,9,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,7,10,12,17	2,4,6,9,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,7,10,12,16,18	2,4,6,9,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,7,10,12,17,18	2,4,6,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,7,10,12,16	2,4,6,9,15	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,7,10,12,14,18	2,4,6,9,18	2^{-1}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,7,10,12,14,16,17	2,4,6,9,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,7,10,12,14	2,4,6,9,15	2^{-1}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,7,10,12,14,16,17,18	2,4,6,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,7,10,12,17,18	2,4,6,9,13,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,7,10,12,16	2,4,6,9,13	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,7,10,12,17	2,4,6,9,13,15,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,7,10,12,16,18	2,4,6,9,13,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,7,10,12,14	2,4,6,9,13	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,7,10,12,14,16,17,18	2,4,6,9,13,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,7,10,12,14,18	2,4,6,9,13,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,7,10,12,14,16,17	2,4,6,9,13,15,17	2^{-23}

Table 0.1720 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,7,10	2,4,6,9,11	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,7,10,16,17,18	2,4,6,9,11,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,7,10,18	2,4,6,9,11,15,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,7,10,16,17	2,4,6,9,11,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,7,10,14,17,18	2,4,6,9,11,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,7,10,14,16	2,4,6,9,11	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,7,10,14,17	2,4,6,9,11,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,7,10,14,16,18	2,4,6,9,11,15,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,7,10,18	2,4,6,9,11,13,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,7,10,16,17	2,4,6,9,11,13,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,7,10	2,4,6,9,11,13,15	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,7,10,16,17,18	2,4,6,9,11,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,7,10,14,17	2,4,6,9,11,13,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,7,10,14,16,18	2,4,6,9,11,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,7,10,14,17,18	2,4,6,9,11,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,7,10,14,16	2,4,6,9,11,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,7,10,12,17,18	2,4,6,9,11,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,7,10,12,16	2,4,6,9,11	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,7,10,12,17	2,4,6,9,11,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,7,10,12,16,18	2,4,6,9,11,15,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,7,10,12,14	2,4,6,9,11	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,7,10,12,14,16,17,18	2,4,6,9,11,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,7,10,12,14,18	2,4,6,9,11,15,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,7,10,12,14,16,17	2,4,6,9,11,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,7,10,12,17	2,4,6,9,11,13,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,7,10,12,16,18	2,4,6,9,11,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,7,10,12,17,18	2,4,6,9,11,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,7,10,12,16	2,4,6,9,11,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,7,10,12,14,18	2,4,6,9,11,13,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,7,10,12,14,16,17	2,4,6,9,11,13,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,7,10,12,14	2,4,6,9,11,13,15	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,7,10,12,14,16,17,18	2,4,6,9,11,13,15,17,18	2^{-23}

Table 0.1721 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,7	2,4,6,8	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,7,16,17,18	2,4,6,8,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,7,18	2,4,6,8,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,7,16,17	2,4,6,8,15,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,7,14,17,18	2,4,6,8,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,7,14,16	2,4,6,8	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,7,14,17	2,4,6,8,15,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,7,14,16,18	2,4,6,8,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,7,18	2,4,6,8,13,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,7,16,17	2,4,6,8,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,7	2,4,6,8,13,15	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,7,16,17,18	2,4,6,8,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,7,14,17	2,4,6,8,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,7,14,16,18	2,4,6,8,13,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,7,14,17,18	2,4,6,8,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,7,14,16	2,4,6,8,13,15	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,7,12,17,18	2,4,6,8,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,7,12,16	2,4,6,8	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,7,12,17	2,4,6,8,15,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,7,12,16,18	2,4,6,8,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,7,12,14	2,4,6,8	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,7,12,14,16,17,18	2,4,6,8,17,18	2^{-1}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,7,12,14,18	2,4,6,8,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,7,12,14,16,17	2,4,6,8,15,17	2^{-1}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,7,12,17	2,4,6,8,13,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,7,12,16,18	2,4,6,8,13,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,7,12,17,18	2,4,6,8,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,7,12,16	2,4,6,8,13,15	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,7,12,14,18	2,4,6,8,13,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,7,12,14,16,17	2,4,6,8,13,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,7,12,14	2,4,6,8,13,15	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,7,12,14,16,17,18	2,4,6,8,13,15,17,18	$2^{-6.5}$

Table 0.1722 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,7,18	2,4,6,8,11,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,7,16,17	2,4,6,8,11,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,7	2,4,6,8,11,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,7,16,17,18	2,4,6,8,11,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,7,14,17	2,4,6,8,11,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,7,14,16,18	2,4,6,8,11,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,7,14,17,18	2,4,6,8,11,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,7,14,16	2,4,6,8,11,15	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,7	2,4,6,8,11,13	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,7,16,17,18	2,4,6,8,11,13,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,7,18	2,4,6,8,11,13,15,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,7,16,17	2,4,6,8,11,13,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,7,14,17,18	2,4,6,8,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,7,14,16	2,4,6,8,11,13	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,7,14,17	2,4,6,8,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,7,14,16,18	2,4,6,8,11,13,15,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,7,12,17	2,4,6,8,11,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,7,12,16,18	2,4,6,8,11,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,7,12,17,18	2,4,6,8,11,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,7,12,16	2,4,6,8,11,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,7,12,14,18	2,4,6,8,11,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,7,12,14,16,17	2,4,6,8,11,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,7,12,14	2,4,6,8,11,15	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,7,12,14,16,17,18	2,4,6,8,11,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,7,12,17,18	2,4,6,8,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,7,12,16	2,4,6,8,11,13	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,7,12,17	2,4,6,8,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,7,12,16,18	2,4,6,8,11,13,15,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,7,12,14	2,4,6,8,11,13	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,7,12,14,16,17,18	2,4,6,8,11,13,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,7,12,14,18	2,4,6,8,11,13,15,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,7,12,14,16,17	2,4,6,8,11,13,15,17	$2^{-6.5}$

Table 0.1723 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,7,10,17,18	2,4,6,8,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,7,10,16	2,4,6,8	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,7,10,17	2,4,6,8,15,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,7,10,16,18	2,4,6,8,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,7,10,14	2,4,6,8	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,7,10,14,16,17,18	2,4,6,8,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,7,10,14,18	2,4,6,8,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,7,10,14,16,17	2,4,6,8,15,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,7,10,17	2,4,6,8,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,7,10,16,18	2,4,6,8,13,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,7,10,17,18	2,4,6,8,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,7,10,16	2,4,6,8,13,15	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,7,10,14,18	2,4,6,8,13,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,7,10,14,16,17	2,4,6,8,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,7,10,14	2,4,6,8,13,15	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,7,10,14,16,17,18	2,4,6,8,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,7,10,12	2,4,6,8	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,7,10,12,16,17,18	2,4,6,8,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,7,10,12,18	2,4,6,8,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,7,10,12,16,17	2,4,6,8,15,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,7,10,12,14,17,18	2,4,6,8,17,18	2^{-34}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,7,10,12,14,16	2,4,6,8	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,7,10,12,14,17	2,4,6,8,15,17	2^{-34}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,7,10,12,14,16,18	2,4,6,8,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,7,10,12,18	2,4,6,8,13,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,7,10,12,16,17	2,4,6,8,13,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,7,10,12	2,4,6,8,13,15	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,7,10,12,16,17,18	2,4,6,8,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,7,10,12,14,17	2,4,6,8,13,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,7,10,12,14,16,18	2,4,6,8,13,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,7,10,12,14,17,18	2,4,6,8,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,7,10,12,14,16	2,4,6,8,13,15	2^{-12}

Table 0.1724 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,7,10,17	2,4,6,8,11,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,7,10,16,18	2,4,6,8,11,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,7,10,17,18	2,4,6,8,11,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,7,10,16	2,4,6,8,11,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,7,10,14,18	2,4,6,8,11,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,7,10,14,16,17	2,4,6,8,11,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,7,10,14	2,4,6,8,11,15	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,7,10,14,16,17,18	2,4,6,8,11,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,7,10,17,18	2,4,6,8,11,13,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,7,10,16	2,4,6,8,11,13	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,7,10,17	2,4,6,8,11,13,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,7,10,16,18	2,4,6,8,11,13,15,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,7,10,14	2,4,6,8,11,13	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,7,10,14,16,17,18	2,4,6,8,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,7,10,14,18	2,4,6,8,11,13,15,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,7,10,14,16,17	2,4,6,8,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,7,10,12,18	2,4,6,8,11,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,7,10,12,16,17	2,4,6,8,11,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,7,10,12	2,4,6,8,11,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,7,10,12,16,17,18	2,4,6,8,11,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,7,10,12,14,17	2,4,6,8,11,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,7,10,12,14,16,18	2,4,6,8,11,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,7,10,12,14,17,18	2,4,6,8,11,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,7,10,12,14,16	2,4,6,8,11,15	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,7,10,12	2,4,6,8,11,13	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,7,10,12,16,17,18	2,4,6,8,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,7,10,12,18	2,4,6,8,11,13,15,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,7,10,12,16,17	2,4,6,8,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,7,10,12,14,17,18	2,4,6,8,11,13,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,7,10,12,14,16	2,4,6,8,11,13	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,7,10,12,14,17	2,4,6,8,11,13,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,7,10,12,14,16,18	2,4,6,8,11,13,15,18	2^{-12}

Table 0.1725 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,7,18	2,4,6,8,9,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,7,16,17	2,4,6,8,9,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,7	2,4,6,8,9,15	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,7,16,17,18	2,4,6,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,7,14,17	2,4,6,8,9,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,7,14,16,18	2,4,6,8,9,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,7,14,17,18	2,4,6,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,7,14,16	2,4,6,8,9,15	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,7	2,4,6,8,9,13	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,7,16,17,18	2,4,6,8,9,13,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,7,18	2,4,6,8,9,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,7,16,17	2,4,6,8,9,13,15,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,7,14,17,18	2,4,6,8,9,13,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,7,14,16	2,4,6,8,9,13	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,7,14,17	2,4,6,8,9,13,15,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,7,14,16,18	2,4,6,8,9,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,7,12,17	2,4,6,8,9,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,7,12,16,18	2,4,6,8,9,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,7,12,17,18	2,4,6,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,7,12,16	2,4,6,8,9,15	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,7,12,14,18	2,4,6,8,9,18	2^{-34}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,7,12,14,16,17	2,4,6,8,9,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,7,12,14	2,4,6,8,9,15	2^{-34}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,7,12,14,16,17,18	2,4,6,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,7,12,17,18	2,4,6,8,9,13,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,7,12,16	2,4,6,8,9,13	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,7,12,17	2,4,6,8,9,13,15,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,7,12,16,18	2,4,6,8,9,13,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,7,12,14	2,4,6,8,9,13	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,7,12,14,16,17,18	2,4,6,8,9,13,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,7,12,14,18	2,4,6,8,9,13,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,7,12,14,16,17	2,4,6,8,9,13,15,17	2^{-12}

Table 0.1726 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,7	2,4,6,8,9,11	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,7,16,17,18	2,4,6,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,7,18	2,4,6,8,9,11,15,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,7,16,17	2,4,6,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,7,14,17,18	2,4,6,8,9,11,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,7,14,16	2,4,6,8,9,11	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,7,14,17	2,4,6,8,9,11,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,7,14,16,18	2,4,6,8,9,11,15,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,7,18	2,4,6,8,9,11,13,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,7,16,17	2,4,6,8,9,11,13,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,7	2,4,6,8,9,11,13,15	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,7,16,17,18	2,4,6,8,9,11,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,7,14,17	2,4,6,8,9,11,13,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,7,14,16,18	2,4,6,8,9,11,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,7,14,17,18	2,4,6,8,9,11,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,7,14,16	2,4,6,8,9,11,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,7,12,17,18	2,4,6,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,7,12,16	2,4,6,8,9,11	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,7,12,17	2,4,6,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,7,12,16,18	2,4,6,8,9,11,15,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,7,12,14	2,4,6,8,9,11	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,7,12,14,16,17,18	2,4,6,8,9,11,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,7,12,14,18	2,4,6,8,9,11,15,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,7,12,14,16,17	2,4,6,8,9,11,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,7,12,17	2,4,6,8,9,11,13,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,7,12,16,18	2,4,6,8,9,11,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,7,12,17,18	2,4,6,8,9,11,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,7,12,16	2,4,6,8,9,11,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,7,12,14,18	2,4,6,8,9,11,13,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,7,12,14,16,17	2,4,6,8,9,11,13,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,7,12,14	2,4,6,8,9,11,13,15	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,7,12,14,16,17,18	2,4,6,8,9,11,13,15,17,18	2^{-12}

Table 0.1727 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,7,10,17	2,4,6,8,9,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,7,10,16,18	2,4,6,8,9,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,7,10,17,18	2,4,6,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,7,10,16	2,4,6,8,9,15	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,7,10,14,18	2,4,6,8,9,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,7,10,14,16,17	2,4,6,8,9,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,7,10,14	2,4,6,8,9,15	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,7,10,14,16,17,18	2,4,6,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,7,10,17,18	2,4,6,8,9,13,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,7,10,16	2,4,6,8,9,13	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,7,10,17	2,4,6,8,9,13,15,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,7,10,16,18	2,4,6,8,9,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,7,10,14	2,4,6,8,9,13	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,7,10,14,16,17,18	2,4,6,8,9,13,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,7,10,14,18	2,4,6,8,9,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,7,10,14,16,17	2,4,6,8,9,13,15,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,7,10,12,18	2,4,6,8,9,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,7,10,12,16,17	2,4,6,8,9,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,7,10,12	2,4,6,8,9,15	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,7,10,12,16,17,18	2,4,6,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,7,10,12,14,17	2,4,6,8,9,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,7,10,12,14,16,18	2,4,6,8,9,18	2^{-1}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,7,10,12,14,17,18	2,4,6,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,7,10,12,14,16	2,4,6,8,9,15	2^{-1}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,7,10,12	2,4,6,8,9,13	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,7,10,12,16,17,18	2,4,6,8,9,13,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,7,10,12,18	2,4,6,8,9,13,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,7,10,12,16,17	2,4,6,8,9,13,15,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,7,10,12,14,17,18	2,4,6,8,9,13,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,7,10,12,14,16	2,4,6,8,9,13	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,7,10,12,14,17	2,4,6,8,9,13,15,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,7,10,12,14,16,18	2,4,6,8,9,13,15,18	$2^{-6.5}$

Table 0.1728 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,7,10,17,18	2,4,6,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,7,10,16	2,4,6,8,9,11	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,7,10,17	2,4,6,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,7,10,16,18	2,4,6,8,9,11,15,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,7,10,14	2,4,6,8,9,11	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,7,10,14,16,17,18	2,4,6,8,9,11,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,7,10,14,18	2,4,6,8,9,11,15,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,7,10,14,16,17	2,4,6,8,9,11,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,7,10,17	2,4,6,8,9,11,13,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,7,10,16,18	2,4,6,8,9,11,13,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,7,10,17,18	2,4,6,8,9,11,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,7,10,16	2,4,6,8,9,11,13,15	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,7,10,14,18	2,4,6,8,9,11,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,7,10,14,16,17	2,4,6,8,9,11,13,17	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,7,10,14	2,4,6,8,9,11,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,7,10,14,16,17,18	2,4,6,8,9,11,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,7,10,12	2,4,6,8,9,11	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,7,10,12,16,17,18	2,4,6,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,7,10,12,18	2,4,6,8,9,11,15,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,7,10,12,16,17	2,4,6,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,7,10,12,14,17,18	2,4,6,8,9,11,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,7,10,12,14,16	2,4,6,8,9,11	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,7,10,12,14,17	2,4,6,8,9,11,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,7,10,12,14,16,18	2,4,6,8,9,11,15,18	2^{-12}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,7,10,12,18	2,4,6,8,9,11,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,7,10,12,16,17	2,4,6,8,9,11,13,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,7,10,12	2,4,6,8,9,11,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,7,10,12,16,17,18	2,4,6,8,9,11,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,7,10,12,14,17	2,4,6,8,9,11,13,17	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,7,10,12,14,16,18	2,4,6,8,9,11,13,18	$2^{-6.5}$
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,7,10,12,14,17,18	2,4,6,8,9,11,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,7,10,12,14,16	2,4,6,8,9,11,13,15	$2^{-6.5}$

Table 0.1729 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,5	2,4	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,16,17,18	2,4,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,5,18	2,4,15,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,16,17	2,4,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,5,14,17,18	2,4,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,5,14,16	2,4	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,5,14,17	2,4,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,5,14,16,18	2,4,15,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,5,18	2,4,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,5,16,17	2,4,13,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,5	2,4,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,5,16,17,18	2,4,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,5,14,17	2,4,13,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,5,14,16,18	2,4,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,5,14,17,18	2,4,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,5,14,16	2,4,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,5,12,17,18	2,4,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,5,12,16	2,4	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,5,12,17	2,4,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,5,12,16,18	2,4,15,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,5,12,14	2,4	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,5,12,14,16,17,18	2,4,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,5,12,14,18	2,4,15,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,5,12,14,16,17	2,4,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,5,12,17	2,4,13,17	2^{-1}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,5,12,16,18	2,4,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,5,12,17,18	2,4,13,15,17,18	2^{-1}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,5,12,16	2,4,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,5,12,14,18	2,4,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,12,14,16,17	2,4,13,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,5,12,14	2,4,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,5,12,14,16,17,18	2,4,13,15,17,18	2^{-12}

Table 0.1730 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,5,18	2,4,11,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,16,17	2,4,11,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,5	2,4,11,15	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,16,17,18	2,4,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,5,14,17	2,4,11,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,5,14,16,18	2,4,11,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,5,14,17,18	2,4,11,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,5,14,16	2,4,11,15	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,5	2,4,11,13	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,5,16,17,18	2,4,11,13,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,5,18	2,4,11,13,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,5,16,17	2,4,11,13,15,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,14,17,18	2,4,11,13,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,5,14,16	2,4,11,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,14,17	2,4,11,13,15,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,5,14,16,18	2,4,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,5,12,17	2,4,11,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,5,12,16,18	2,4,11,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,5,12,17,18	2,4,11,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,5,12,16	2,4,11,15	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,5,12,14,18	2,4,11,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,5,12,14,16,17	2,4,11,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,5,12,14	2,4,11,15	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,5,12,14,16,17,18	2,4,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,5,12,17,18	2,4,11,13,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,5,12,16	2,4,11,13	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,5,12,17	2,4,11,13,15,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,5,12,16,18	2,4,11,13,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0)$	1,5,12,14	2,4,11,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,5,12,14,16,17,18	2,4,11,13,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,5,12,14,18	2,4,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,5,12,14,16,17	2,4,11,13,15,17	2^{-12}

Table 0.1731 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,5,10,17,18	2,4,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,5,10,16	2,4	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,5,10,17	2,4,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,5,10,16,18	2,4,15,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,5,10,14	2,4	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,5,10,14,16,17,18	2,4,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,5,10,14,18	2,4,15,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,5,10,14,16,17	2,4,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,5,10,17	2,4,13,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,5,10,16,18	2,4,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,5,10,17,18	2,4,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,5,10,16	2,4,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,5,10,14,18	2,4,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,5,10,14,16,17	2,4,13,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,5,10,14	2,4,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,5,10,14,16,17,18	2,4,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,5,10,12	2,4	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,5,10,12,16,17,18	2,4,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,5,10,12,18	2,4,15,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,5,10,12,16,17	2,4,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,5,10,12,14,17,18	2,4,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,5,10,12,14,16	2,4	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,5,10,12,14,17	2,4,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,5,10,12,14,16,18	2,4,15,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,5,10,12,18	2,4,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,5,10,12,16,17	2,4,13,17	2^{-34}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,5,10,12	2,4,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,5,10,12,16,17,18	2,4,13,15,17,18	2^{-34}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,5,10,12,14,17	2,4,13,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,5,10,12,14,16,18	2,4,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,5,10,12,14,17,18	2,4,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,5,10,12,14,16	2,4,13,15	$2^{-17.5}$

Table 0.1732 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,5,10,17	2,4,11,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,5,10,16,18	2,4,11,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,5,10,17,18	2,4,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,5,10,16	2,4,11,15	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,5,10,14,18	2,4,11,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,5,10,14,16,17	2,4,11,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,5,10,14	2,4,11,15	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,5,10,14,16,17,18	2,4,11,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,5,10,17,18	2,4,11,13,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,5,10,16	2,4,11,13	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,5,10,17	2,4,11,13,15,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,5,10,16,18	2,4,11,13,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,5,10,14	2,4,11,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,5,10,14,16,17,18	2,4,11,13,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,5,10,14,18	2,4,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,5,10,14,16,17	2,4,11,13,15,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,5,10,12,18	2,4,11,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,5,10,12,16,17	2,4,11,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,5,10,12	2,4,11,15	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,5,10,12,16,17,18	2,4,11,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,5,10,12,14,17	2,4,11,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,5,10,12,14,16,18	2,4,11,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,5,10,12,14,17,18	2,4,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,5,10,12,14,16	2,4,11,15	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,5,10,12	2,4,11,13	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,5,10,12,16,17,18	2,4,11,13,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,5,10,12,18	2,4,11,13,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,5,10,12,16,17	2,4,11,13,15,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,5,10,12,14,17,18	2,4,11,13,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,5,10,12,14,16	2,4,11,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,5,10,12,14,17	2,4,11,13,15,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,5,10,12,14,16,18	2,4,11,13,15,18	$2^{-17.5}$

Table 0.1733 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,5,18	2,4,9,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,5,16,17	2,4,9,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,5	2,4,9,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,5,16,17,18	2,4,9,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,14,17	2,4,9,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,5,14,16,18	2,4,9,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,14,17,18	2,4,9,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,5,14,16	2,4,9,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,5	2,4,9,13	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,5,16,17,18	2,4,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,5,18	2,4,9,13,15,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,5,16,17	2,4,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,5,14,17,18	2,4,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,5,14,16	2,4,9,13	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,5,14,17	2,4,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,5,14,16,18	2,4,9,13,15,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,5,12,17	2,4,9,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,5,12,16,18	2,4,9,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,5,12,17,18	2,4,9,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1)$	1,5,12,16	2,4,9,15	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,5,12,14,18	2,4,9,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,5,12,14,16,17	2,4,9,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,5,12,14	2,4,9,15	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,5,12,14,16,17,18	2,4,9,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,5,12,17,18	2,4,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,12,16	2,4,9,13	2^{-34}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,5,12,17	2,4,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,12,16,18	2,4,9,13,15,18	2^{-34}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,5,12,14	2,4,9,13	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,5,12,14,16,17,18	2,4,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,5,12,14,18	2,4,9,13,15,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,5,12,14,16,17	2,4,9,13,15,17	$2^{-17.5}$

Table 0.1734 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,5	2,4,9,11	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,5,16,17,18	2,4,9,11,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,5,18	2,4,9,11,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,5,16,17	2,4,9,11,15,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,5,14,17,18	2,4,9,11,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,5,14,16	2,4,9,11	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,5,14,17	2,4,9,11,15,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,5,14,16,18	2,4,9,11,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,18	2,4,9,11,13,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,5,16,17	2,4,9,11,13,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5	2,4,9,11,13,15	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,5,16,17,18	2,4,9,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,5,14,17	2,4,9,11,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,5,14,16,18	2,4,9,11,13,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,5,14,17,18	2,4,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,5,14,16	2,4,9,11,13,15	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,5,12,17,18	2,4,9,11,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,5,12,16	2,4,9,11	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,5,12,17	2,4,9,11,15,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,5,12,16,18	2,4,9,11,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,5,12,14	2,4,9,11	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,5,12,14,16,17,18	2,4,9,11,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,5,12,14,18	2,4,9,11,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,5,12,14,16,17	2,4,9,11,15,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,5,12,17	2,4,9,11,13,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,5,12,16,18	2,4,9,11,13,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,5,12,17,18	2,4,9,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,5,12,16	2,4,9,11,13,15	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,5,12,14,18	2,4,9,11,13,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,5,12,14,16,17	2,4,9,11,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,5,12,14	2,4,9,11,13,15	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,5,12,14,16,17,18	2,4,9,11,13,15,17,18	$2^{-17.5}$

Table 0.1735 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,10,17	2,4,9,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,10,16,18	2,4,9,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,10,17,18	2,4,9,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,10,16	2,4,9,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,5,10,14,18	2,4,9,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,5,10,14,16,17	2,4,9,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,5,10,14	2,4,9,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,5,10,14,16,17,18	2,4,9,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,5,10,17,18	2,4,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,5,10,16	2,4,9,13	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,5,10,17	2,4,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,5,10,16,18	2,4,9,13,15,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,5,10,14	2,4,9,13	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,5,10,14,16,17,18	2,4,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,5,10,14,18	2,4,9,13,15,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,5,10,14,16,17	2,4,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,5,10,12,18	2,4,9,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,5,10,12,16,17	2,4,9,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,5,10,12	2,4,9,15	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,5,10,12,16,17,18	2,4,9,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,5,10,12,14,17	2,4,9,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,5,10,12,14,16,18	2,4,9,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,5,10,12,14,17,18	2,4,9,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,5,10,12,14,16	2,4,9,15	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,5,10,12	2,4,9,13	2^{-1}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,5,10,12,16,17,18	2,4,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,5,10,12,18	2,4,9,13,15,18	2^{-1}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,5,10,12,16,17	2,4,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,5,10,12,14,17,18	2,4,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,5,10,12,14,16	2,4,9,13	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,5,10,12,14,17	2,4,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,5,10,12,14,16,18	2,4,9,13,15,18	2^{-12}

Table 0.1736 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,5,10,17,18	2,4,9,11,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,5,10,16	2,4,9,11	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,5,10,17	2,4,9,11,15,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,5,10,16,18	2,4,9,11,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,5,10,14	2,4,9,11	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,5,10,14,16,17,18	2,4,9,11,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,5,10,14,18	2,4,9,11,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,5,10,14,16,17	2,4,9,11,15,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,5,10,17	2,4,9,11,13,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,5,10,16,18	2,4,9,11,13,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,10,17,18	2,4,9,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,5,10,16	2,4,9,11,13,15	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,5,10,14,18	2,4,9,11,13,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,10,14,16,17	2,4,9,11,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,5,10,14	2,4,9,11,13,15	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,5,10,14,16,17,18	2,4,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,5,10,12	2,4,9,11	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,5,10,12,16,17,18	2,4,9,11,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,5,10,12,18	2,4,9,11,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,5,10,12,16,17	2,4,9,11,15,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,5,10,12,14,17,18	2,4,9,11,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,5,10,12,14,16	2,4,9,11	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,5,10,12,14,17	2,4,9,11,15,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,5,10,12,14,16,18	2,4,9,11,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,5,10,12,18	2,4,9,11,13,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,10,12,16,17	2,4,9,11,13,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,5,10,12	2,4,9,11,13,15	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,10,12,16,17,18	2,4,9,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,5,10,12,14,17	2,4,9,11,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,5,10,12,14,16,18	2,4,9,11,13,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,5,10,12,14,17,18	2,4,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,5,10,12,14,16	2,4,9,11,13,15	2^{-12}

Table 0.1737 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,17,18	2,4,8,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,16	2,4,8	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,17	2,4,8,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,16,18	2,4,8,15,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,5,14	2,4,8	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,5,14,16,17,18	2,4,8,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,5,14,18	2,4,8,15,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,5,14,16,17	2,4,8,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,5,17	2,4,8,13,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,5,16,18	2,4,8,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,5,17,18	2,4,8,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,5,16	2,4,8,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,5,14,18	2,4,8,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,5,14,16,17	2,4,8,13,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,5,14	2,4,8,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,5,14,16,17,18	2,4,8,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,5,12	2,4,8	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,5,12,16,17,18	2,4,8,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,5,12,18	2,4,8,15,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,5,12,16,17	2,4,8,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,5,12,14,17,18	2,4,8,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,5,12,14,16	2,4,8	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,5,12,14,17	2,4,8,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,5,12,14,16,18	2,4,8,15,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,5,12,18	2,4,8,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,5,12,16,17	2,4,8,13,17	2^{-1}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,5,12	2,4,8,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,5,12,16,17,18	2,4,8,13,15,17,18	2^{-1}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,12,14,17	2,4,8,13,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,5,12,14,16,18	2,4,8,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,5,12,14,17,18	2,4,8,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,5,12,14,16	2,4,8,13,15	$2^{-17.5}$

Table 0.1738 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,5,17	2,4,8,11,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,5,16,18	2,4,8,11,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,5,17,18	2,4,8,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,5,16	2,4,8,11,15	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,5,14,18	2,4,8,11,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,5,14,16,17	2,4,8,11,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,5,14	2,4,8,11,15	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,5,14,16,17,18	2,4,8,11,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,5,17,18	2,4,8,11,13,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,5,16	2,4,8,11,13	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,5,17	2,4,8,11,13,15,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,5,16,18	2,4,8,11,13,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,5,14	2,4,8,11,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,5,14,16,17,18	2,4,8,11,13,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,5,14,18	2,4,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,5,14,16,17	2,4,8,11,13,15,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,5,12,18	2,4,8,11,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,5,12,16,17	2,4,8,11,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,5,12	2,4,8,11,15	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,5,12,16,17,18	2,4,8,11,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,5,12,14,17	2,4,8,11,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,5,12,14,16,18	2,4,8,11,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,5,12,14,17,18	2,4,8,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,5,12,14,16	2,4,8,11,15	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,12	2,4,8,11,13	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,5,12,16,17,18	2,4,8,11,13,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,12,18	2,4,8,11,13,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,5,12,16,17	2,4,8,11,13,15,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,5,12,14,17,18	2,4,8,11,13,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,5,12,14,16	2,4,8,11,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,5,12,14,17	2,4,8,11,13,15,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,5,12,14,16,18	2,4,8,11,13,15,18	$2^{-17.5}$

Table 0.1739 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,5,10	2,4,8	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,5,10,16,17,18	2,4,8,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,5,10,18	2,4,8,15,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,5,10,16,17	2,4,8,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,5,10,14,17,18	2,4,8,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,10,14,16	2,4,8	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,5,10,14,17	2,4,8,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,10,14,16,18	2,4,8,15,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,5,10,18	2,4,8,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,5,10,16,17	2,4,8,13,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,10	2,4,8,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,5,10,16,17,18	2,4,8,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,5,10,14,17	2,4,8,13,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,10,14,16,18	2,4,8,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,5,10,14,17,18	2,4,8,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,10,14,16	2,4,8,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,5,10,12,17,18	2,4,8,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,5,10,12,16	2,4,8	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,5,10,12,17	2,4,8,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,5,10,12,16,18	2,4,8,15,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,5,10,12,14	2,4,8	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,5,10,12,14,16,17,18	2,4,8,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,5,10,12,14,18	2,4,8,15,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,5,10,12,14,16,17	2,4,8,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,10,12,17	2,4,8,13,17	2^{-34}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,5,10,12,16,18	2,4,8,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,10,12,17,18	2,4,8,13,15,17,18	2^{-34}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,5,10,12,16	2,4,8,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,5,10,12,14,18	2,4,8,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,10,12,14,16,17	2,4,8,13,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,5,10,12,14	2,4,8,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,5,10,12,14,16,17,18	2,4,8,13,15,17,18	2^{-23}

Table 0.1740 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,5,10,18	2,4,8,11,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,5,10,16,17	2,4,8,11,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,5,10	2,4,8,11,15	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,5,10,16,17,18	2,4,8,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,5,10,14,17	2,4,8,11,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,5,10,14,16,18	2,4,8,11,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,5,10,14,17,18	2,4,8,11,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,5,10,14,16	2,4,8,11,15	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,5,10	2,4,8,11,13	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,10,16,17,18	2,4,8,11,13,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,5,10,18	2,4,8,11,13,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,10,16,17	2,4,8,11,13,15,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,5,10,14,17,18	2,4,8,11,13,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,5,10,14,16	2,4,8,11,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,5,10,14,17	2,4,8,11,13,15,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,5,10,14,16,18	2,4,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,5,10,12,17	2,4,8,11,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,5,10,12,16,18	2,4,8,11,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,5,10,12,17,18	2,4,8,11,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,5,10,12,16	2,4,8,11,15	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,5,10,12,14,18	2,4,8,11,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,5,10,12,14,16,17	2,4,8,11,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,5,10,12,14	2,4,8,11,15	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,5,10,12,14,16,17,18	2,4,8,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,5,10,12,17,18	2,4,8,11,13,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,5,10,12,16	2,4,8,11,13	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,5,10,12,17	2,4,8,11,13,15,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,5,10,12,16,18	2,4,8,11,13,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,5,10,12,14	2,4,8,11,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,5,10,12,14,16,17,18	2,4,8,11,13,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,5,10,12,14,18	2,4,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,5,10,12,14,16,17	2,4,8,11,13,15,17	2^{-23}

Table 0.1741 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,5,17	2,4,8,9,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,5,16,18	2,4,8,9,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,5,17,18	2,4,8,9,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,5,16	2,4,8,9,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,5,14,18	2,4,8,9,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,5,14,16,17	2,4,8,9,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,5,14	2,4,8,9,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,5,14,16,17,18	2,4,8,9,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,5,17,18	2,4,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,5,16	2,4,8,9,13	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,5,17	2,4,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,5,16,18	2,4,8,9,13,15,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,5,14	2,4,8,9,13	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,5,14,16,17,18	2,4,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,5,14,18	2,4,8,9,13,15,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,5,14,16,17	2,4,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,5,12,18	2,4,8,9,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,5,12,16,17	2,4,8,9,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,5,12	2,4,8,9,15	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,5,12,16,17,18	2,4,8,9,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,5,12,14,17	2,4,8,9,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,5,12,14,16,18	2,4,8,9,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,5,12,14,17,18	2,4,8,9,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,5,12,14,16	2,4,8,9,15	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,5,12	2,4,8,9,13	2^{-34}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,5,12,16,17,18	2,4,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,5,12,18	2,4,8,9,13,15,18	2^{-34}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,5,12,16,17	2,4,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,5,12,14,17,18	2,4,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,5,12,14,16	2,4,8,9,13	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,5,12,14,17	2,4,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,5,12,14,16,18	2,4,8,9,13,15,18	2^{-23}

Table 0.1742 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,5,17,18	2,4,8,9,11,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,5,16	2,4,8,9,11	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,5,17	2,4,8,9,11,15,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,5,16,18	2,4,8,9,11,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,5,14	2,4,8,9,11	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,5,14,16,17,18	2,4,8,9,11,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,5,14,18	2,4,8,9,11,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,5,14,16,17	2,4,8,9,11,15,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,5,17	2,4,8,9,11,13,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,5,16,18	2,4,8,9,11,13,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,5,17,18	2,4,8,9,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,5,16	2,4,8,9,11,13,15	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,5,14,18	2,4,8,9,11,13,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,5,14,16,17	2,4,8,9,11,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,5,14	2,4,8,9,11,13,15	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,5,14,16,17,18	2,4,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,5,12	2,4,8,9,11	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,5,12,16,17,18	2,4,8,9,11,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,5,12,18	2,4,8,9,11,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,5,12,16,17	2,4,8,9,11,15,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,5,12,14,17,18	2,4,8,9,11,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,5,12,14,16	2,4,8,9,11	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,5,12,14,17	2,4,8,9,11,15,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,5,12,14,16,18	2,4,8,9,11,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,5,12,18	2,4,8,9,11,13,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,5,12,16,17	2,4,8,9,11,13,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,5,12	2,4,8,9,11,13,15	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,5,12,16,17,18	2,4,8,9,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,5,12,14,17	2,4,8,9,11,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,5,12,14,16,18	2,4,8,9,11,13,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,5,12,14,17,18	2,4,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,5,12,14,16	2,4,8,9,11,13,15	2^{-23}

Table 0.1743 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,10,18	2,4,8,9,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,5,10,16,17	2,4,8,9,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,10	2,4,8,9,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,5,10,16,17,18	2,4,8,9,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,5,10,14,17	2,4,8,9,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,5,10,14,16,18	2,4,8,9,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,5,10,14,17,18	2,4,8,9,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,5,10,14,16	2,4,8,9,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,5,10	2,4,8,9,13	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,5,10,16,17,18	2,4,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,5,10,18	2,4,8,9,13,15,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,5,10,16,17	2,4,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,5,10,14,17,18	2,4,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,5,10,14,16	2,4,8,9,13	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,5,10,14,17	2,4,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,5,10,14,16,18	2,4,8,9,13,15,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,5,10,12,17	2,4,8,9,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,5,10,12,16,18	2,4,8,9,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,5,10,12,17,18	2,4,8,9,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,5,10,12,16	2,4,8,9,15	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,5,10,12,14,18	2,4,8,9,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,5,10,12,14,16,17	2,4,8,9,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,5,10,12,14	2,4,8,9,15	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,5,10,12,14,16,17,18	2,4,8,9,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,5,10,12,17,18	2,4,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,5,10,12,16	2,4,8,9,13	2^{-1}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,5,10,12,17	2,4,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,5,10,12,16,18	2,4,8,9,13,15,18	2^{-1}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,5,10,12,14	2,4,8,9,13	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,5,10,12,14,16,17,18	2,4,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,5,10,12,14,18	2,4,8,9,13,15,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,5,10,12,14,16,17	2,4,8,9,13,15,17	$2^{-17.5}$

Table 0.1744 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,10	2,4,8,9,11	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,5,10,16,17,18	2,4,8,9,11,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,10,18	2,4,8,9,11,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,5,10,16,17	2,4,8,9,11,15,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,5,10,14,17,18	2,4,8,9,11,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,5,10,14,16	2,4,8,9,11	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,5,10,14,17	2,4,8,9,11,15,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,5,10,14,16,18	2,4,8,9,11,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,5,10,18	2,4,8,9,11,13,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,5,10,16,17	2,4,8,9,11,13,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,5,10	2,4,8,9,11,13,15	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0)$	1,5,10,16,17,18	2,4,8,9,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,5,10,14,17	2,4,8,9,11,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,10,14,16,18	2,4,8,9,11,13,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,5,10,14,17,18	2,4,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,10,14,16	2,4,8,9,11,13,15	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,5,10,12,17,18	2,4,8,9,11,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,5,10,12,16	2,4,8,9,11	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,5,10,12,17	2,4,8,9,11,15,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,5,10,12,16,18	2,4,8,9,11,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,5,10,12,14	2,4,8,9,11	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,5,10,12,14,16,17,18	2,4,8,9,11,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,5,10,12,14,18	2,4,8,9,11,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,5,10,12,14,16,17	2,4,8,9,11,15,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,5,10,12,17	2,4,8,9,11,13,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,5,10,12,16,18	2,4,8,9,11,13,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,5,10,12,17,18	2,4,8,9,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,5,10,12,16	2,4,8,9,11,13,15	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,5,10,12,14,18	2,4,8,9,11,13,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,5,10,12,14,16,17	2,4,8,9,11,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,5,10,12,14	2,4,8,9,11,13,15	2^{-12}
$(1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,5,10,12,14,16,17,18	2,4,8,9,11,13,15,17,18	$2^{-17.5}$

Table 0.1745 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,5,7,18	2,4,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,5,7,16,17	2,4,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,5,7	2,4,15	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,5,7,16,17,18	2,4,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,5,7,14,17	2,4,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,5,7,14,16,18	2,4,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,5,7,14,17,18	2,4,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,5,7,14,16	2,4,15	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,7	2,4,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,5,7,16,17,18	2,4,13,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,7,18	2,4,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,5,7,16,17	2,4,13,15,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,5,7,14,17,18	2,4,13,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,5,7,14,16	2,4,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,5,7,14,17	2,4,13,15,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,5,7,14,16,18	2,4,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,5,7,12,17	2,4,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,5,7,12,16,18	2,4,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,5,7,12,17,18	2,4,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,5,7,12,16	2,4,15	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,5,7,12,14,18	2,4,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,5,7,12,14,16,17	2,4,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,5,7,12,14	2,4,15	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,5,7,12,14,16,17,18	2,4,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,5,7,12,17,18	2,4,13,17,18	2^{-1}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,7,12,16	2,4,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,5,7,12,17	2,4,13,15,17	2^{-1}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,5,7,12,16,18	2,4,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,5,7,12,14	2,4,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,5,7,12,14,16,17,18	2,4,13,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,5,7,12,14,18	2,4,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,5,7,12,14,16,17	2,4,13,15,17	2^{-12}

Table 0.1746 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,5,7	2,4,11	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,5,7,16,17,18	2,4,11,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,5,7,18	2,4,11,15,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,5,7,16,17	2,4,11,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,14,17,18	2,4,11,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,5,7,14,16	2,4,11	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,14,17	2,4,11,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,5,7,14,16,18	2,4,11,15,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,5,7,18	2,4,11,13,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,5,7,16,17	2,4,11,13,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,5,7	2,4,11,13,15	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,5,7,16,17,18	2,4,11,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,5,7,14,17	2,4,11,13,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0)$	1,5,7,14,16,18	2,4,11,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,5,7,14,17,18	2,4,11,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,5,7,14,16	2,4,11,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,12,17,18	2,4,11,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,12,16	2,4,11	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,12,17	2,4,11,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,12,16,18	2,4,11,15,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,5,7,12,14	2,4,11	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,5,7,12,14,16,17,18	2,4,11,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,5,7,12,14,18	2,4,11,15,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,5,7,12,14,16,17	2,4,11,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,5,7,12,17	2,4,11,13,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,7,12,16,18	2,4,11,13,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,5,7,12,17,18	2,4,11,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,7,12,16	2,4,11,13,15	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,5,7,12,14,18	2,4,11,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,5,7,12,14,16,17	2,4,11,13,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,5,7,12,14	2,4,11,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,5,7,12,14,16,17,18	2,4,11,13,15,17,18	2^{-12}

Table 0.1747 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,5,7,10,17	2,4,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,5,7,10,16,18	2,4,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,5,7,10,17,18	2,4,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,5,7,10,16	2,4,15	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,5,7,10,14,18	2,4,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,5,7,10,14,16,17	2,4,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,5,7,10,14	2,4,15	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,5,7,10,14,16,17,18	2,4,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,5,7,10,17,18	2,4,13,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,5,7,10,16	2,4,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,5,7,10,17	2,4,13,15,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,5,7,10,16,18	2,4,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,5,7,10,14	2,4,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,5,7,10,14,16,17,18	2,4,13,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,5,7,10,14,18	2,4,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,5,7,10,14,16,17	2,4,13,15,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,5,7,10,12,18	2,4,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,5,7,10,12,16,17	2,4,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,5,7,10,12	2,4,15	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,5,7,10,12,16,17,18	2,4,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,5,7,10,12,14,17	2,4,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,5,7,10,12,14,16,18	2,4,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,5,7,10,12,14,17,18	2,4,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,5,7,10,12,14,16	2,4,15	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,5,7,10,12	2,4,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,7,10,12,16,17,18	2,4,13,17,18	2^{-34}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,5,7,10,12,18	2,4,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,7,10,12,16,17	2,4,13,15,17	2^{-34}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,5,7,10,12,14,17,18	2,4,13,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,5,7,10,12,14,16	2,4,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,5,7,10,12,14,17	2,4,13,15,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,5,7,10,12,14,16,18	2,4,13,15,18	$2^{-17.5}$

Table 0.1748 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,10,17,18	2,4,11,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,10,16	2,4,11	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,10,17	2,4,11,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,10,16,18	2,4,11,15,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,10,14	2,4,11	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,5,7,10,14,16,17,18	2,4,11,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,10,14,18	2,4,11,15,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,5,7,10,14,16,17	2,4,11,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,10,17	2,4,11,13,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,5,7,10,16,18	2,4,11,13,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,10,17,18	2,4,11,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,5,7,10,16	2,4,11,13,15	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,5,7,10,14,18	2,4,11,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,5,7,10,14,16,17	2,4,11,13,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,5,7,10,14	2,4,11,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,5,7,10,14,16,17,18	2,4,11,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,5,7,10,12	2,4,11	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,5,7,10,12,16,17,18	2,4,11,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,5,7,10,12,18	2,4,11,15,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,5,7,10,12,16,17	2,4,11,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,5,7,10,12,14,17,18	2,4,11,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,5,7,10,12,14,16	2,4,11	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,5,7,10,12,14,17	2,4,11,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,5,7,10,12,14,16,18	2,4,11,15,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,5,7,10,12,18	2,4,11,13,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,5,7,10,12,16,17	2,4,11,13,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,5,7,10,12	2,4,11,13,15	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,5,7,10,12,16,17,18	2,4,11,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,5,7,10,12,14,17	2,4,11,13,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,5,7,10,12,14,16,18	2,4,11,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,5,7,10,12,14,17,18	2,4,11,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,5,7,10,12,14,16	2,4,11,13,15	$2^{-17.5}$

Table 0.1749 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,5,7	2,4,9	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,7,16,17,18	2,4,9,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,5,7,18	2,4,9,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,7,16,17	2,4,9,15,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,5,7,14,17,18	2,4,9,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,5,7,14,16	2,4,9	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,5,7,14,17	2,4,9,15,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,5,7,14,16,18	2,4,9,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,5,7,18	2,4,9,13,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,5,7,16,17	2,4,9,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,5,7	2,4,9,13,15	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,5,7,16,17,18	2,4,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,14,17	2,4,9,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,5,7,14,16,18	2,4,9,13,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,14,17,18	2,4,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,5,7,14,16	2,4,9,13,15	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,5,7,12,17,18	2,4,9,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,5,7,12,16	2,4,9	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,5,7,12,17	2,4,9,15,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,5,7,12,16,18	2,4,9,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,5,7,12,14	2,4,9	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,5,7,12,14,16,17,18	2,4,9,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,5,7,12,14,18	2,4,9,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,5,7,12,14,16,17	2,4,9,15,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,5,7,12,17	2,4,9,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,5,7,12,16,18	2,4,9,13,18	2^{-34}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,5,7,12,17,18	2,4,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,5,7,12,16	2,4,9,13,15	2^{-34}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,5,7,12,14,18	2,4,9,13,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,5,7,12,14,16,17	2,4,9,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,5,7,12,14	2,4,9,13,15	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,5,7,12,14,16,17,18	2,4,9,13,15,17,18	$2^{-17.5}$

Table 0.1750 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,5,7,18	2,4,9,11,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,7,16,17	2,4,9,11,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,5,7	2,4,9,11,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,7,16,17,18	2,4,9,11,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,5,7,14,17	2,4,9,11,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,5,7,14,16,18	2,4,9,11,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,5,7,14,17,18	2,4,9,11,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,5,7,14,16	2,4,9,11,15	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,5,7	2,4,9,11,13	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,5,7,16,17,18	2,4,9,11,13,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,5,7,18	2,4,9,11,13,15,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,5,7,16,17	2,4,9,11,13,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,5,7,14,17,18	2,4,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,5,7,14,16	2,4,9,11,13	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,5,7,14,17	2,4,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,5,7,14,16,18	2,4,9,11,13,15,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,5,7,12,17	2,4,9,11,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,5,7,12,16,18	2,4,9,11,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,5,7,12,17,18	2,4,9,11,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,5,7,12,16	2,4,9,11,15	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,5,7,12,14,18	2,4,9,11,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,5,7,12,14,16,17	2,4,9,11,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0)$	1,5,7,12,14	2,4,9,11,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,5,7,12,14,16,17,18	2,4,9,11,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,5,7,12,17,18	2,4,9,11,13,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,5,7,12,16	2,4,9,11,13	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,5,7,12,17	2,4,9,11,13,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,5,7,12,16,18	2,4,9,11,13,15,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,5,7,12,14	2,4,9,11,13	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,5,7,12,14,16,17,18	2,4,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,5,7,12,14,18	2,4,9,11,13,15,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,5,7,12,14,16,17	2,4,9,11,13,15,17	$2^{-17.5}$

Table 0.1751 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,5,7,10,17,18	2,4,9,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,5,7,10,16	2,4,9	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,5,7,10,17	2,4,9,15,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,5,7,10,16,18	2,4,9,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,5,7,10,14	2,4,9	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,5,7,10,14,16,17,18	2,4,9,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,5,7,10,14,18	2,4,9,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,5,7,10,14,16,17	2,4,9,15,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,5,7,10,17	2,4,9,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,5,7,10,16,18	2,4,9,13,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,5,7,10,17,18	2,4,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,5,7,10,16	2,4,9,13,15	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,5,7,10,14,18	2,4,9,13,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,5,7,10,14,16,17	2,4,9,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,5,7,10,14	2,4,9,13,15	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,5,7,10,14,16,17,18	2,4,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,5,7,10,12	2,4,9	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,5,7,10,12,16,17,18	2,4,9,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,5,7,10,12,18	2,4,9,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,5,7,10,12,16,17	2,4,9,15,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,5,7,10,12,14,17,18	2,4,9,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,5,7,10,12,14,16	2,4,9	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,5,7,10,12,14,17	2,4,9,15,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,5,7,10,12,14,16,18	2,4,9,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,5,7,10,12,18	2,4,9,13,18	2^{-1}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,5,7,10,12,16,17	2,4,9,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,5,7,10,12	2,4,9,13,15	2^{-1}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,5,7,10,12,16,17,18	2,4,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,5,7,10,12,14,17	2,4,9,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,5,7,10,12,14,16,18	2,4,9,13,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,5,7,10,12,14,17,18	2,4,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,5,7,10,12,14,16	2,4,9,13,15	2^{-12}

Table 0.1752 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,5,7,10,17	2,4,9,11,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,5,7,10,16,18	2,4,9,11,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,5,7,10,17,18	2,4,9,11,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,5,7,10,16	2,4,9,11,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,5,7,10,14,18	2,4,9,11,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,5,7,10,14,16,17	2,4,9,11,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,5,7,10,14	2,4,9,11,15	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,5,7,10,14,16,17,18	2,4,9,11,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,5,7,10,17,18	2,4,9,11,13,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,5,7,10,16	2,4,9,11,13	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,5,7,10,17	2,4,9,11,13,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,5,7,10,16,18	2,4,9,11,13,15,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,5,7,10,14	2,4,9,11,13	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,5,7,10,14,16,17,18	2,4,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,5,7,10,14,18	2,4,9,11,13,15,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,5,7,10,14,16,17	2,4,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,5,7,10,12,18	2,4,9,11,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,5,7,10,12,16,17	2,4,9,11,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,5,7,10,12	2,4,9,11,15	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,5,7,10,12,16,17,18	2,4,9,11,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,10,12,14,17	2,4,9,11,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,5,7,10,12,14,16,18	2,4,9,11,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,10,12,14,17,18	2,4,9,11,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,5,7,10,12,14,16	2,4,9,11,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,5,7,10,12	2,4,9,11,13	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,5,7,10,12,16,17,18	2,4,9,11,13,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,5,7,10,12,18	2,4,9,11,13,15,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,5,7,10,12,16,17	2,4,9,11,13,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,7,10,12,14,17,18	2,4,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,5,7,10,12,14,16	2,4,9,11,13	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,7,10,12,14,17	2,4,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,5,7,10,12,14,16,18	2,4,9,11,13,15,18	2^{-12}

Table 0.1753 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,5,7,17	2,4,8,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,5,7,16,18	2,4,8,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,5,7,17,18	2,4,8,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,5,7,16	2,4,8,15	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,5,7,14,18	2,4,8,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,5,7,14,16,17	2,4,8,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,5,7,14	2,4,8,15	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,5,7,14,16,17,18	2,4,8,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,5,7,17,18	2,4,8,13,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,5,7,16	2,4,8,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,5,7,17	2,4,8,13,15,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,5,7,16,18	2,4,8,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,5,7,14	2,4,8,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,5,7,14,16,17,18	2,4,8,13,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,5,7,14,18	2,4,8,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,5,7,14,16,17	2,4,8,13,15,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,5,7,12,18	2,4,8,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,5,7,12,16,17	2,4,8,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,5,7,12	2,4,8,15	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,5,7,12,16,17,18	2,4,8,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,5,7,12,14,17	2,4,8,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,5,7,12,14,16,18	2,4,8,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,5,7,12,14,17,18	2,4,8,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,5,7,12,14,16	2,4,8,15	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,5,7,12	2,4,8,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,5,7,12,16,17,18	2,4,8,13,17,18	2^{-1}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,5,7,12,18	2,4,8,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,5,7,12,16,17	2,4,8,13,15,17	2^{-1}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,5,7,12,14,17,18	2,4,8,13,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,5,7,12,14,16	2,4,8,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,5,7,12,14,17	2,4,8,13,15,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,5,7,12,14,16,18	2,4,8,13,15,18	$2^{-17.5}$

Table 0.1754 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,5,7,17,18	2,4,8,11,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,5,7,16	2,4,8,11	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,5,7,17	2,4,8,11,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,5,7,16,18	2,4,8,11,15,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,5,7,14	2,4,8,11	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,5,7,14,16,17,18	2,4,8,11,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,5,7,14,18	2,4,8,11,15,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,5,7,14,16,17	2,4,8,11,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,5,7,17	2,4,8,11,13,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,5,7,16,18	2,4,8,11,13,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,5,7,17,18	2,4,8,11,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,16	2,4,8,11,13,15	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,5,7,14,18	2,4,8,11,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,5,7,14,16,17	2,4,8,11,13,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,5,7,14	2,4,8,11,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,5,7,14,16,17,18	2,4,8,11,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,5,7,12	2,4,8,11	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0)$	1,5,7,12,16,17,18	2,4,8,11,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,5,7,12,18	2,4,8,11,15,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,5,7,12,16,17	2,4,8,11,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,5,7,12,14,17,18	2,4,8,11,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,12,14,16	2,4,8,11	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,5,7,12,14,17	2,4,8,11,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,12,14,16,18	2,4,8,11,15,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,5,7,12,18	2,4,8,11,13,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,5,7,12,16,17	2,4,8,11,13,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,5,7,12	2,4,8,11,13,15	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,5,7,12,16,17,18	2,4,8,11,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,5,7,12,14,17	2,4,8,11,13,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,7,12,14,16,18	2,4,8,11,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1)$	1,5,7,12,14,17,18	2,4,8,11,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,7,12,14,16	2,4,8,11,13,15	$2^{-17.5}$

Table 0.1755 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,7,10,18	2,4,8,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,5,7,10,16,17	2,4,8,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,7,10	2,4,8,15	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,5,7,10,16,17,18	2,4,8,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,5,7,10,14,17	2,4,8,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,5,7,10,14,16,18	2,4,8,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,5,7,10,14,17,18	2,4,8,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,5,7,10,14,16	2,4,8,15	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,5,7,10	2,4,8,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,5,7,10,16,17,18	2,4,8,13,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,5,7,10,18	2,4,8,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,5,7,10,16,17	2,4,8,13,15,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,5,7,10,14,17,18	2,4,8,13,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,10,14,16	2,4,8,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,5,7,10,14,17	2,4,8,13,15,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,10,14,16,18	2,4,8,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,5,7,10,12,17	2,4,8,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,5,7,10,12,16,18	2,4,8,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,5,7,10,12,17,18	2,4,8,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,5,7,10,12,16	2,4,8,15	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,5,7,10,12,14,18	2,4,8,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,5,7,10,12,14,16,17	2,4,8,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,5,7,10,12,14	2,4,8,15	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,5,7,10,12,14,16,17,18	2,4,8,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,5,7,10,12,17,18	2,4,8,13,17,18	2^{-34}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,5,7,10,12,16	2,4,8,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,5,7,10,12,17	2,4,8,13,15,17	2^{-34}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,5,7,10,12,16,18	2,4,8,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,5,7,10,12,14	2,4,8,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,5,7,10,12,14,16,17,18	2,4,8,13,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,5,7,10,12,14,18	2,4,8,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,5,7,10,12,14,16,17	2,4,8,13,15,17	2^{-23}

Table 0.1756 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,7,10	2,4,8,11	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,5,7,10,16,17,18	2,4,8,11,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,7,10,18	2,4,8,11,15,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,5,7,10,16,17	2,4,8,11,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,5,7,10,14,17,18	2,4,8,11,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,5,7,10,14,16	2,4,8,11	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,5,7,10,14,17	2,4,8,11,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,5,7,10,14,16,18	2,4,8,11,15,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,5,7,10,18	2,4,8,11,13,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,5,7,10,16,17	2,4,8,11,13,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,5,7,10	2,4,8,11,13,15	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,5,7,10,16,17,18	2,4,8,11,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,5,7,10,14,17	2,4,8,11,13,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,10,14,16,18	2,4,8,11,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,5,7,10,14,17,18	2,4,8,11,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,5,7,10,14,16	2,4,8,11,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,5,7,10,12,17,18	2,4,8,11,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,5,7,10,12,16	2,4,8,11	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,5,7,10,12,17	2,4,8,11,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,5,7,10,12,16,18	2,4,8,11,15,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,5,7,10,12,14	2,4,8,11	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,5,7,10,12,14,16,17,18	2,4,8,11,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,5,7,10,12,14,18	2,4,8,11,15,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,5,7,10,12,14,16,17	2,4,8,11,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,5,7,10,12,17	2,4,8,11,13,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,5,7,10,12,16,18	2,4,8,11,13,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,5,7,10,12,17,18	2,4,8,11,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,5,7,10,12,16	2,4,8,11,13,15	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,5,7,10,12,14,18	2,4,8,11,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,5,7,10,12,14,16,17	2,4,8,11,13,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,5,7,10,12,14	2,4,8,11,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,5,7,10,12,14,16,17,18	2,4,8,11,13,15,17,18	2^{-23}

Table 0.1757 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,5,7,17,18	2,4,8,9,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,5,7,16	2,4,8,9	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,5,7,17	2,4,8,9,15,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,5,7,16,18	2,4,8,9,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,5,7,14	2,4,8,9	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,5,7,14,16,17,18	2,4,8,9,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,5,7,14,18	2,4,8,9,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,5,7,14,16,17	2,4,8,9,15,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,5,7,17	2,4,8,9,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,5,7,16,18	2,4,8,9,13,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,5,7,17,18	2,4,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,5,7,16	2,4,8,9,13,15	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,5,7,14,18	2,4,8,9,13,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,5,7,14,16,17	2,4,8,9,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,7,14	2,4,8,9,13,15	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,5,7,14,16,17,18	2,4,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,5,7,12	2,4,8,9	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,5,7,12,16,17,18	2,4,8,9,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,5,7,12,18	2,4,8,9,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,5,7,12,16,17	2,4,8,9,15,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,5,7,12,14,17,18	2,4,8,9,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,5,7,12,14,16	2,4,8,9	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,5,7,12,14,17	2,4,8,9,15,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,5,7,12,14,16,18	2,4,8,9,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,7,12,18	2,4,8,9,13,18	2^{-34}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,5,7,12,16,17	2,4,8,9,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,7,12	2,4,8,9,13,15	2^{-34}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,5,7,12,16,17,18	2,4,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,5,7,12,14,17	2,4,8,9,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,5,7,12,14,16,18	2,4,8,9,13,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,5,7,12,14,17,18	2,4,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,5,7,12,14,16	2,4,8,9,13,15	2^{-23}

Table 0.1758 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,17	2,4,8,9,11,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,16,18	2,4,8,9,11,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,17,18	2,4,8,9,11,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,16	2,4,8,9,11,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,5,7,14,18	2,4,8,9,11,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,14,16,17	2,4,8,9,11,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,5,7,14	2,4,8,9,11,15	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,14,16,17,18	2,4,8,9,11,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,5,7,17,18	2,4,8,9,11,13,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,16	2,4,8,9,11,13	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,5,7,17	2,4,8,9,11,13,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,16,18	2,4,8,9,11,13,15,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,5,7,14	2,4,8,9,11,13	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,5,7,14,16,17,18	2,4,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,5,7,14,18	2,4,8,9,11,13,15,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,5,7,14,16,17	2,4,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,5,7,12,18	2,4,8,9,11,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,5,7,12,16,17	2,4,8,9,11,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,5,7,12	2,4,8,9,11,15	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,5,7,12,16,17,18	2,4,8,9,11,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,5,7,12,14,17	2,4,8,9,11,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,5,7,12,14,16,18	2,4,8,9,11,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,5,7,12,14,17,18	2,4,8,9,11,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,5,7,12,14,16	2,4,8,9,11,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,5,7,12	2,4,8,9,11,13	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,5,7,12,16,17,18	2,4,8,9,11,13,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,5,7,12,18	2,4,8,9,11,13,15,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,5,7,12,16,17	2,4,8,9,11,13,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,5,7,12,14,17,18	2,4,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,5,7,12,14,16	2,4,8,9,11,13	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,5,7,12,14,17	2,4,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,5,7,12,14,16,18	2,4,8,9,11,13,15,18	2^{-23}

Table 0.1759 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,5,7,10	2,4,8,9	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,5,7,10,16,17,18	2,4,8,9,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,5,7,10,18	2,4,8,9,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,5,7,10,16,17	2,4,8,9,15,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,5,7,10,14,17,18	2,4,8,9,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,10,14,16	2,4,8,9	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,5,7,10,14,17	2,4,8,9,15,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,5,7,10,14,16,18	2,4,8,9,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,5,7,10,18	2,4,8,9,13,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,7,10,16,17	2,4,8,9,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,5,7,10	2,4,8,9,13,15	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,7,10,16,17,18	2,4,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,5,7,10,14,17	2,4,8,9,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,5,7,10,14,16,18	2,4,8,9,13,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,5,7,10,14,17,18	2,4,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,10,14,16	2,4,8,9,13,15	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,5,7,10,12,17,18	2,4,8,9,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,10,12,16	2,4,8,9	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,5,7,10,12,17	2,4,8,9,15,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,5,7,10,12,16,18	2,4,8,9,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,5,7,10,12,14	2,4,8,9	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,5,7,10,12,14,16,17,18	2,4,8,9,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,5,7,10,12,14,18	2,4,8,9,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,5,7,10,12,14,16,17	2,4,8,9,15,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,5,7,10,12,17	2,4,8,9,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,5,7,10,12,16,18	2,4,8,9,13,18	2^{-1}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,5,7,10,12,17,18	2,4,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,5,7,10,12,16	2,4,8,9,13,15	2^{-1}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,5,7,10,12,14,18	2,4,8,9,13,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,5,7,10,12,14,16,17	2,4,8,9,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,5,7,10,12,14	2,4,8,9,13,15	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,5,7,10,12,14,16,17,18	2,4,8,9,13,15,17,18	$2^{-17.5}$

Table 0.1760 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,5,7,10,18	2,4,8,9,11,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,5,7,10,16,17	2,4,8,9,11,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,5,7,10	2,4,8,9,11,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,5,7,10,16,17,18	2,4,8,9,11,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,5,7,10,14,17	2,4,8,9,11,17	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,10,14,16,18	2,4,8,9,11,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,5,7,10,14,17,18	2,4,8,9,11,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,5,7,10,14,16	2,4,8,9,11,15	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,5,7,10	2,4,8,9,11,13	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,5,7,10,16,17,18	2,4,8,9,11,13,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,5,7,10,18	2,4,8,9,11,13,15,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,5,7,10,16,17	2,4,8,9,11,13,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,10,14,17,18	2,4,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,5,7,10,14,16	2,4,8,9,11,13	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,5,7,10,14,17	2,4,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,10,14,16,18	2,4,8,9,11,13,15,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,10,12,17	2,4,8,9,11,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,10,12,16,18	2,4,8,9,11,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,10,12,17,18	2,4,8,9,11,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,10,12,16	2,4,8,9,11,15	$2^{-6.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,5,7,10,12,14,18	2,4,8,9,11,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,5,7,10,12,14,16,17	2,4,8,9,11,17	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,5,7,10,12,14	2,4,8,9,11,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,5,7,10,12,14,16,17,18	2,4,8,9,11,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,7,10,12,17,18	2,4,8,9,11,13,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,5,7,10,12,16	2,4,8,9,11,13	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,7,10,12,17	2,4,8,9,11,13,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,5,7,10,12,16,18	2,4,8,9,11,13,15,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,5,7,10,12,14	2,4,8,9,11,13	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,5,7,10,12,14,16,17,18	2,4,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,5,7,10,12,14,18	2,4,8,9,11,13,15,18	2^{-12}
$(1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,5,7,10,12,14,16,17	2,4,8,9,11,13,15,17	$2^{-17.5}$

Table 0.1761 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,5,17,18	2,4,6,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,5,16	2,4,6	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,5,17	2,4,6,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,5,16,18	2,4,6,15,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,5,14	2,4,6	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,5,14,16,17,18	2,4,6,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,5,14,18	2,4,6,15,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,5,14,16,17	2,4,6,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,5,17	2,4,6,13,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,5,16,18	2,4,6,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,5,17,18	2,4,6,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,5,16	2,4,6,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,5,14,18	2,4,6,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,5,14,16,17	2,4,6,13,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,5,14	2,4,6,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,5,14,16,17,18	2,4,6,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,5,12	2,4,6	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,5,12,16,17,18	2,4,6,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,5,12,18	2,4,6,15,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,5,12,16,17	2,4,6,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,5,12,14,17,18	2,4,6,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,5,12,14,16	2,4,6	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,5,12,14,17	2,4,6,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,5,12,14,16,18	2,4,6,15,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,5,12,18	2,4,6,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,5,12,16,17	2,4,6,13,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,5,12	2,4,6,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,5,12,16,17,18	2,4,6,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,5,12,14,17	2,4,6,13,17	2^{-1}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,5,12,14,16,18	2,4,6,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,5,12,14,17,18	2,4,6,13,15,17,18	2^{-1}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,5,12,14,16	2,4,6,13,15	$2^{-17.5}$

Table 0.1762 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,5,17	2,4,6,11,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,5,16,18	2,4,6,11,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,5,17,18	2,4,6,11,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,5,16	2,4,6,11,15	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,5,14,18	2,4,6,11,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,5,14,16,17	2,4,6,11,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,5,14	2,4,6,11,15	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,5,14,16,17,18	2,4,6,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,5,17,18	2,4,6,11,13,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,5,16	2,4,6,11,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,5,17	2,4,6,11,13,15,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,5,16,18	2,4,6,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,5,14	2,4,6,11,13	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,5,14,16,17,18	2,4,6,11,13,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,5,14,18	2,4,6,11,13,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,5,14,16,17	2,4,6,11,13,15,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,5,12,18	2,4,6,11,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,5,12,16,17	2,4,6,11,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,5,12	2,4,6,11,15	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,5,12,16,17,18	2,4,6,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,5,12,14,17	2,4,6,11,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,5,12,14,16,18	2,4,6,11,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,5,12,14,17,18	2,4,6,11,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,5,12,14,16	2,4,6,11,15	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,5,12	2,4,6,11,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,5,12,16,17,18	2,4,6,11,13,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,5,12,18	2,4,6,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,5,12,16,17	2,4,6,11,13,15,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,5,12,14,17,18	2,4,6,11,13,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,5,12,14,16	2,4,6,11,13	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,5,12,14,17	2,4,6,11,13,15,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,5,12,14,16,18	2,4,6,11,13,15,18	$2^{-28.5}$

Table 0.1763 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,5,10	2,4,6	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,5,10,16,17,18	2,4,6,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,5,10,18	2,4,6,15,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,5,10,16,17	2,4,6,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,5,10,14,17,18	2,4,6,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,5,10,14,16	2,4,6	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,5,10,14,17	2,4,6,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1)$	1,5,10,14,16,18	2,4,6,15,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,5,10,18	2,4,6,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,5,10,16,17	2,4,6,13,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,5,10	2,4,6,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,5,10,16,17,18	2,4,6,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,5,10,14,17	2,4,6,13,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,5,10,14,16,18	2,4,6,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,5,10,14,17,18	2,4,6,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,5,10,14,16	2,4,6,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,5,10,12,17,18	2,4,6,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,5,10,12,16	2,4,6	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,5,10,12,17	2,4,6,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,5,10,12,16,18	2,4,6,15,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,5,10,12,14	2,4,6	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,10,12,14,16,17,18	2,4,6,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,5,10,12,14,18	2,4,6,15,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,10,12,14,16,17	2,4,6,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,5,10,12,17	2,4,6,13,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,5,10,12,16,18	2,4,6,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,5,10,12,17,18	2,4,6,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,5,10,12,16	2,4,6,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,5,10,12,14,18	2,4,6,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,5,10,12,14,16,17	2,4,6,13,17	2^{-34}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,5,10,12,14	2,4,6,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,5,10,12,14,16,17,18	2,4,6,13,15,17,18	2^{-34}

Table 0.1764 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,5,10,18	2,4,6,11,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,5,10,16,17	2,4,6,11,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,5,10	2,4,6,11,15	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,5,10,16,17,18	2,4,6,11,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,5,10,14,17	2,4,6,11,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,5,10,14,16,18	2,4,6,11,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,5,10,14,17,18	2,4,6,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,5,10,14,16	2,4,6,11,15	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,5,10	2,4,6,11,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,5,10,16,17,18	2,4,6,11,13,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,5,10,18	2,4,6,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,5,10,16,17	2,4,6,11,13,15,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,5,10,14,17,18	2,4,6,11,13,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,5,10,14,16	2,4,6,11,13	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,5,10,14,17	2,4,6,11,13,15,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,5,10,14,16,18	2,4,6,11,13,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,5,10,12,17	2,4,6,11,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,5,10,12,16,18	2,4,6,11,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,5,10,12,17,18	2,4,6,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,5,10,12,16	2,4,6,11,15	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,5,10,12,14,18	2,4,6,11,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,10,12,14,16,17	2,4,6,11,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,5,10,12,14	2,4,6,11,15	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,10,12,14,16,17,18	2,4,6,11,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,10,12,17,18	2,4,6,11,13,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,5,10,12,16	2,4,6,11,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,10,12,17	2,4,6,11,13,15,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,5,10,12,16,18	2,4,6,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,5,10,12,14	2,4,6,11,13	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,5,10,12,14,16,17,18	2,4,6,11,13,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,5,10,12,14,18	2,4,6,11,13,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,5,10,12,14,16,17	2,4,6,11,13,15,17	2^{-23}

Table 0.1765 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,5,17	2,4,6,9,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,5,16,18	2,4,6,9,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,5,17,18	2,4,6,9,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,5,16	2,4,6,9,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,5,14,18	2,4,6,9,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,5,14,16,17	2,4,6,9,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,5,14	2,4,6,9,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,5,14,16,17,18	2,4,6,9,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,5,17,18	2,4,6,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,5,16	2,4,6,9,13	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,5,17	2,4,6,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,5,16,18	2,4,6,9,13,15,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,5,14	2,4,6,9,13	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,5,14,16,17,18	2,4,6,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,5,14,18	2,4,6,9,13,15,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,5,14,16,17	2,4,6,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,5,12,18	2,4,6,9,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,5,12,16,17	2,4,6,9,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,5,12	2,4,6,9,15	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,5,12,16,17,18	2,4,6,9,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,5,12,14,17	2,4,6,9,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,12,14,16,18	2,4,6,9,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,12,14,17,18	2,4,6,9,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,12,14,16	2,4,6,9,15	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,5,12	2,4,6,9,13	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,5,12,16,17,18	2,4,6,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,5,12,18	2,4,6,9,13,15,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,5,12,16,17	2,4,6,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,5,12,14,17,18	2,4,6,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,5,12,14,16	2,4,6,9,13	2^{-34}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,5,12,14,17	2,4,6,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,5,12,14,16,18	2,4,6,9,13,15,18	2^{-34}

Table 0.1766 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,5,17,18	2,4,6,9,11,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,5,16	2,4,6,9,11	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,5,17	2,4,6,9,11,15,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,5,16,18	2,4,6,9,11,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,5,14	2,4,6,9,11	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,5,14,16,17,18	2,4,6,9,11,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,5,14,18	2,4,6,9,11,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,5,14,16,17	2,4,6,9,11,15,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,5,17	2,4,6,9,11,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,5,16,18	2,4,6,9,11,13,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,5,17,18	2,4,6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,5,16	2,4,6,9,11,13,15	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,5,14,18	2,4,6,9,11,13,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,14,16,17	2,4,6,9,11,13,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,5,14	2,4,6,9,11,13,15	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,14,16,17,18	2,4,6,9,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,5,12	2,4,6,9,11	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,5,12,16,17,18	2,4,6,9,11,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,5,12,18	2,4,6,9,11,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,5,12,16,17	2,4,6,9,11,15,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,5,12,14,17,18	2,4,6,9,11,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,5,12,14,16	2,4,6,9,11	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,5,12,14,17	2,4,6,9,11,15,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,5,12,14,16,18	2,4,6,9,11,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,5,12,18	2,4,6,9,11,13,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,5,12,16,17	2,4,6,9,11,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,5,12	2,4,6,9,11,13,15	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,5,12,16,17,18	2,4,6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,5,12,14,17	2,4,6,9,11,13,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,5,12,14,16,18	2,4,6,9,11,13,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,5,12,14,17,18	2,4,6,9,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,5,12,14,16	2,4,6,9,11,13,15	2^{-23}

Table 0.1767 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,5,10,18	2,4,6,9,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,5,10,16,17	2,4,6,9,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,5,10	2,4,6,9,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,5,10,16,17,18	2,4,6,9,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,5,10,14,17	2,4,6,9,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,5,10,14,16,18	2,4,6,9,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,5,10,14,17,18	2,4,6,9,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,5,10,14,16	2,4,6,9,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,5,10	2,4,6,9,13	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,5,10,16,17,18	2,4,6,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,5,10,18	2,4,6,9,13,15,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,5,10,16,17	2,4,6,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,5,10,14,17,18	2,4,6,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,10,14,16	2,4,6,9,13	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,5,10,14,17	2,4,6,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,10,14,16,18	2,4,6,9,13,15,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,10,12,17	2,4,6,9,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,5,10,12,16,18	2,4,6,9,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,10,12,17,18	2,4,6,9,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,5,10,12,16	2,4,6,9,15	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,5,10,12,14,18	2,4,6,9,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,5,10,12,14,16,17	2,4,6,9,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,5,10,12,14	2,4,6,9,15	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,5,10,12,14,16,17,18	2,4,6,9,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,5,10,12,17,18	2,4,6,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,5,10,12,16	2,4,6,9,13	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,5,10,12,17	2,4,6,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,5,10,12,16,18	2,4,6,9,13,15,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,5,10,12,14	2,4,6,9,13	2^{-1}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,5,10,12,14,16,17,18	2,4,6,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,5,10,12,14,18	2,4,6,9,13,15,18	2^{-1}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,5,10,12,14,16,17	2,4,6,9,13,15,17	$2^{-17.5}$

Table 0.1768 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,5,10	2,4,6,9,11	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,5,10,16,17,18	2,4,6,9,11,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,5,10,18	2,4,6,9,11,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,5,10,16,17	2,4,6,9,11,15,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,5,10,14,17,18	2,4,6,9,11,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,5,10,14,16	2,4,6,9,11	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,5,10,14,17	2,4,6,9,11,15,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,5,10,14,16,18	2,4,6,9,11,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,5,10,18	2,4,6,9,11,13,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,5,10,16,17	2,4,6,9,11,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,5,10	2,4,6,9,11,13,15	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,5,10,16,17,18	2,4,6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,5,10,14,17	2,4,6,9,11,13,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,5,10,14,16,18	2,4,6,9,11,13,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,5,10,14,17,18	2,4,6,9,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,5,10,14,16	2,4,6,9,11,13,15	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,5,10,12,17,18	2,4,6,9,11,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,5,10,12,16	2,4,6,9,11	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,5,10,12,17	2,4,6,9,11,15,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,5,10,12,16,18	2,4,6,9,11,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,10,12,14	2,4,6,9,11	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,5,10,12,14,16,17,18	2,4,6,9,11,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,10,12,14,18	2,4,6,9,11,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,5,10,12,14,16,17	2,4,6,9,11,15,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,5,10,12,17	2,4,6,9,11,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,5,10,12,16,18	2,4,6,9,11,13,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,5,10,12,17,18	2,4,6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,5,10,12,16	2,4,6,9,11,13,15	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,10,12,14,18	2,4,6,9,11,13,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,5,10,12,14,16,17	2,4,6,9,11,13,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,10,12,14	2,4,6,9,11,13,15	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,5,10,12,14,16,17,18	2,4,6,9,11,13,15,17,18	$2^{-28.5}$

Table 0.1769 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,5	2,4,6,8	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,5,16,17,18	2,4,6,8,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,5,18	2,4,6,8,15,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,5,16,17	2,4,6,8,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,5,14,17,18	2,4,6,8,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,5,14,16	2,4,6,8	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,5,14,17	2,4,6,8,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,5,14,16,18	2,4,6,8,15,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,5,18	2,4,6,8,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,5,16,17	2,4,6,8,13,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,5	2,4,6,8,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,5,16,17,18	2,4,6,8,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,14,17	2,4,6,8,13,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,5,14,16,18	2,4,6,8,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,14,17,18	2,4,6,8,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,5,14,16	2,4,6,8,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,5,12,17,18	2,4,6,8,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,12,16	2,4,6,8	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,5,12,17	2,4,6,8,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,12,16,18	2,4,6,8,15,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,5,12,14	2,4,6,8	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,5,12,14,16,17,18	2,4,6,8,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,5,12,14,18	2,4,6,8,15,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,5,12,14,16,17	2,4,6,8,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,5,12,17	2,4,6,8,13,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,5,12,16,18	2,4,6,8,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,5,12,17,18	2,4,6,8,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,5,12,16	2,4,6,8,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,5,12,14,18	2,4,6,8,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,5,12,14,16,17	2,4,6,8,13,17	2^{-1}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,5,12,14	2,4,6,8,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,5,12,14,16,17,18	2,4,6,8,13,15,17,18	2^{-1}

Table 0.1770 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,5,18	2,4,6,8,11,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,5,16,17	2,4,6,8,11,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,5	2,4,6,8,11,15	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,5,16,17,18	2,4,6,8,11,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,5,14,17	2,4,6,8,11,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,5,14,16,18	2,4,6,8,11,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,5,14,17,18	2,4,6,8,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,5,14,16	2,4,6,8,11,15	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,5	2,4,6,8,11,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,5,16,17,18	2,4,6,8,11,13,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,5,18	2,4,6,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,5,16,17	2,4,6,8,11,13,15,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,5,14,17,18	2,4,6,8,11,13,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,5,14,16	2,4,6,8,11,13	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,5,14,17	2,4,6,8,11,13,15,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,5,14,16,18	2,4,6,8,11,13,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,5,12,17	2,4,6,8,11,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,5,12,16,18	2,4,6,8,11,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,5,12,17,18	2,4,6,8,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,5,12,16	2,4,6,8,11,15	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,5,12,14,18	2,4,6,8,11,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,5,12,14,16,17	2,4,6,8,11,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,5,12,14	2,4,6,8,11,15	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,5,12,14,16,17,18	2,4,6,8,11,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,5,12,17,18	2,4,6,8,11,13,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,5,12,16	2,4,6,8,11,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,5,12,17	2,4,6,8,11,13,15,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,5,12,16,18	2,4,6,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,5,12,14	2,4,6,8,11,13	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,12,14,16,17,18	2,4,6,8,11,13,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,5,12,14,18	2,4,6,8,11,13,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,12,14,16,17	2,4,6,8,11,13,15,17	2^{-12}

Table 0.1771 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,5,10,17,18	2,4,6,8,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,5,10,16	2,4,6,8	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,5,10,17	2,4,6,8,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,5,10,16,18	2,4,6,8,15,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,5,10,14	2,4,6,8	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,5,10,14,16,17,18	2,4,6,8,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,5,10,14,18	2,4,6,8,15,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,5,10,14,16,17	2,4,6,8,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,5,10,17	2,4,6,8,13,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,5,10,16,18	2,4,6,8,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,5,10,17,18	2,4,6,8,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,5,10,16	2,4,6,8,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,5,10,14,18	2,4,6,8,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,5,10,14,16,17	2,4,6,8,13,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,5,10,14	2,4,6,8,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,5,10,14,16,17,18	2,4,6,8,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,5,10,12	2,4,6,8	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,5,10,12,16,17,18	2,4,6,8,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,5,10,12,18	2,4,6,8,15,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,5,10,12,16,17	2,4,6,8,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,10,12,14,17,18	2,4,6,8,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,10,12,14,16	2,4,6,8	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,10,12,14,17	2,4,6,8,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,10,12,14,16,18	2,4,6,8,15,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,5,10,12,18	2,4,6,8,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,5,10,12,16,17	2,4,6,8,13,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,5,10,12	2,4,6,8,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,5,10,12,16,17,18	2,4,6,8,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,5,10,12,14,17	2,4,6,8,13,17	2^{-34}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,5,10,12,14,16,18	2,4,6,8,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,5,10,12,14,17,18	2,4,6,8,13,15,17,18	2^{-34}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,5,10,12,14,16	2,4,6,8,13,15	$2^{-17.5}$

Table 0.1772 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,5,10,17	2,4,6,8,11,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,5,10,16,18	2,4,6,8,11,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,5,10,17,18	2,4,6,8,11,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,5,10,16	2,4,6,8,11,15	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,5,10,14,18	2,4,6,8,11,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,5,10,14,16,17	2,4,6,8,11,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,5,10,14	2,4,6,8,11,15	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,5,10,14,16,17,18	2,4,6,8,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,5,10,17,18	2,4,6,8,11,13,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,5,10,16	2,4,6,8,11,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,5,10,17	2,4,6,8,11,13,15,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,5,10,16,18	2,4,6,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,10,14	2,4,6,8,11,13	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,5,10,14,16,17,18	2,4,6,8,11,13,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,10,14,18	2,4,6,8,11,13,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,5,10,14,16,17	2,4,6,8,11,13,15,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,5,10,12,18	2,4,6,8,11,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,5,10,12,16,17	2,4,6,8,11,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,5,10,12	2,4,6,8,11,15	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,5,10,12,16,17,18	2,4,6,8,11,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,5,10,12,14,17	2,4,6,8,11,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,5,10,12,14,16,18	2,4,6,8,11,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,5,10,12,14,17,18	2,4,6,8,11,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,5,10,12,14,16	2,4,6,8,11,15	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,5,10,12	2,4,6,8,11,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,5,10,12,16,17,18	2,4,6,8,11,13,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,5,10,12,18	2,4,6,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,5,10,12,16,17	2,4,6,8,11,13,15,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,5,10,12,14,17,18	2,4,6,8,11,13,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,5,10,12,14,16	2,4,6,8,11,13	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,5,10,12,14,17	2,4,6,8,11,13,15,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,5,10,12,14,16,18	2,4,6,8,11,13,15,18	$2^{-6.5}$

Table 0.1773 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,5,18	2,4,6,8,9,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,5,16,17	2,4,6,8,9,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,5	2,4,6,8,9,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,5,16,17,18	2,4,6,8,9,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,5,14,17	2,4,6,8,9,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,5,14,16,18	2,4,6,8,9,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,5,14,17,18	2,4,6,8,9,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,5,14,16	2,4,6,8,9,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,5	2,4,6,8,9,13	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,5,16,17,18	2,4,6,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,5,18	2,4,6,8,9,13,15,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,5,16,17	2,4,6,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,5,14,17,18	2,4,6,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,5,14,16	2,4,6,8,9,13	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,5,14,17	2,4,6,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,5,14,16,18	2,4,6,8,9,13,15,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,5,12,17	2,4,6,8,9,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,5,12,16,18	2,4,6,8,9,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,5,12,17,18	2,4,6,8,9,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,5,12,16	2,4,6,8,9,15	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,12,14,18	2,4,6,8,9,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,5,12,14,16,17	2,4,6,8,9,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,12,14	2,4,6,8,9,15	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,5,12,14,16,17,18	2,4,6,8,9,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,5,12,17,18	2,4,6,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,5,12,16	2,4,6,8,9,13	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,5,12,17	2,4,6,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,5,12,16,18	2,4,6,8,9,13,15,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,5,12,14	2,4,6,8,9,13	2^{-34}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,5,12,14,16,17,18	2,4,6,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,5,12,14,18	2,4,6,8,9,13,15,18	2^{-34}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,5,12,14,16,17	2,4,6,8,9,13,15,17	$2^{-17.5}$

Table 0.1774 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,5	2,4,6,8,9,11	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,5,16,17,18	2,4,6,8,9,11,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,5,18	2,4,6,8,9,11,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,5,16,17	2,4,6,8,9,11,15,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,5,14,17,18	2,4,6,8,9,11,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,5,14,16	2,4,6,8,9,11	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,5,14,17	2,4,6,8,9,11,15,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,5,14,16,18	2,4,6,8,9,11,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,5,18	2,4,6,8,9,11,13,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,5,16,17	2,4,6,8,9,11,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,5	2,4,6,8,9,11,13,15	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,5,16,17,18	2,4,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,5,14,17	2,4,6,8,9,11,13,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,5,14,16,18	2,4,6,8,9,11,13,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,5,14,17,18	2,4,6,8,9,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,5,14,16	2,4,6,8,9,11,13,15	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,5,12,17,18	2,4,6,8,9,11,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,5,12,16	2,4,6,8,9,11	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,5,12,17	2,4,6,8,9,11,15,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,5,12,16,18	2,4,6,8,9,11,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,12,14	2,4,6,8,9,11	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,5,12,14,16,17,18	2,4,6,8,9,11,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,12,14,18	2,4,6,8,9,11,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,5,12,14,16,17	2,4,6,8,9,11,15,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,5,12,17	2,4,6,8,9,11,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,12,16,18	2,4,6,8,9,11,13,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,5,12,17,18	2,4,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,12,16	2,4,6,8,9,11,13,15	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,5,12,14,18	2,4,6,8,9,11,13,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,5,12,14,16,17	2,4,6,8,9,11,13,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,5,12,14	2,4,6,8,9,11,13,15	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,5,12,14,16,17,18	2,4,6,8,9,11,13,15,17,18	$2^{-6.5}$

Table 0.1775 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,5,10,17	2,4,6,8,9,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,5,10,16,18	2,4,6,8,9,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,5,10,17,18	2,4,6,8,9,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,5,10,16	2,4,6,8,9,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,5,10,14,18	2,4,6,8,9,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,5,10,14,16,17	2,4,6,8,9,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,5,10,14	2,4,6,8,9,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,5,10,14,16,17,18	2,4,6,8,9,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,5,10,17,18	2,4,6,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,5,10,16	2,4,6,8,9,13	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,5,10,17	2,4,6,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,5,10,16,18	2,4,6,8,9,13,15,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,5,10,14	2,4,6,8,9,13	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,5,10,14,16,17,18	2,4,6,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,5,10,14,18	2,4,6,8,9,13,15,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,5,10,14,16,17	2,4,6,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,5,10,12,18	2,4,6,8,9,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,5,10,12,16,17	2,4,6,8,9,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,5,10,12	2,4,6,8,9,15	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,5,10,12,16,17,18	2,4,6,8,9,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,5,10,12,14,17	2,4,6,8,9,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,5,10,12,14,16,18	2,4,6,8,9,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,5,10,12,14,17,18	2,4,6,8,9,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,5,10,12,14,16	2,4,6,8,9,15	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,5,10,12	2,4,6,8,9,13	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,5,10,12,16,17,18	2,4,6,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,5,10,12,18	2,4,6,8,9,13,15,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,5,10,12,16,17	2,4,6,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1)$	1,5,10,12,14,17,18	2,4,6,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,5,10,12,14,16	2,4,6,8,9,13	2^{-1}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,5,10,12,14,17	2,4,6,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,5,10,12,14,16,18	2,4,6,8,9,13,15,18	2^{-1}

Table 0.1776 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,5,10,17,18	2,4,6,8,9,11,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,5,10,16	2,4,6,8,9,11	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,5,10,17	2,4,6,8,9,11,15,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,5,10,16,18	2,4,6,8,9,11,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,5,10,14	2,4,6,8,9,11	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,10,14,16,17,18	2,4,6,8,9,11,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,5,10,14,18	2,4,6,8,9,11,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,5,10,14,16,17	2,4,6,8,9,11,15,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,5,10,17	2,4,6,8,9,11,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,5,10,16,18	2,4,6,8,9,11,13,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,5,10,17,18	2,4,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,5,10,16	2,4,6,8,9,11,13,15	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,5,10,14,18	2,4,6,8,9,11,13,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,5,10,14,16,17	2,4,6,8,9,11,13,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,5,10,14	2,4,6,8,9,11,13,15	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,5,10,14,16,17,18	2,4,6,8,9,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,5,10,12	2,4,6,8,9,11	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,5,10,12,16,17,18	2,4,6,8,9,11,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,5,10,12,18	2,4,6,8,9,11,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,5,10,12,16,17	2,4,6,8,9,11,15,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,5,10,12,14,17,18	2,4,6,8,9,11,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,5,10,12,14,16	2,4,6,8,9,11	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,5,10,12,14,17	2,4,6,8,9,11,15,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,5,10,12,14,16,18	2,4,6,8,9,11,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,5,10,12,18	2,4,6,8,9,11,13,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,5,10,12,16,17	2,4,6,8,9,11,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,5,10,12	2,4,6,8,9,11,13,15	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,5,10,12,16,17,18	2,4,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,5,10,12,14,17	2,4,6,8,9,11,13,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,5,10,12,14,16,18	2,4,6,8,9,11,13,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,5,10,12,14,17,18	2,4,6,8,9,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,5,10,12,14,16	2,4,6,8,9,11,13,15	2^{-12}

Table 0.1777 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,5,7,17	2,4,6,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,5,7,16,18	2,4,6,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,17,18	2,4,6,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,5,7,16	2,4,6,15	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,5,7,14,18	2,4,6,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,5,7,14,16,17	2,4,6,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,5,7,14	2,4,6,15	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,5,7,14,16,17,18	2,4,6,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,5,7,17,18	2,4,6,13,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,5,7,16	2,4,6,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,5,7,17	2,4,6,13,15,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,5,7,16,18	2,4,6,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,5,7,14	2,4,6,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,7,14,16,17,18	2,4,6,13,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,5,7,14,18	2,4,6,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,7,14,16,17	2,4,6,13,15,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,5,7,12,18	2,4,6,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,5,7,12,16,17	2,4,6,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,5,7,12	2,4,6,15	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,5,7,12,16,17,18	2,4,6,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,5,7,12,14,17	2,4,6,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,5,7,12,14,16,18	2,4,6,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,5,7,12,14,17,18	2,4,6,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,5,7,12,14,16	2,4,6,15	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,5,7,12	2,4,6,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,5,7,12,16,17,18	2,4,6,13,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,5,7,12,18	2,4,6,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,5,7,12,16,17	2,4,6,13,15,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,5,7,12,14,17,18	2,4,6,13,17,18	2^{-1}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,5,7,12,14,16	2,4,6,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,5,7,12,14,17	2,4,6,13,15,17	2^{-1}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,5,7,12,14,16,18	2,4,6,13,15,18	$2^{-17.5}$

Table 0.1778 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,5,7,17,18	2,4,6,11,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,5,7,16	2,4,6,11	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,5,7,17	2,4,6,11,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,5,7,16,18	2,4,6,11,15,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,5,7,14	2,4,6,11	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,5,7,14,16,17,18	2,4,6,11,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,5,7,14,18	2,4,6,11,15,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,5,7,14,16,17	2,4,6,11,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,5,7,17	2,4,6,11,13,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,5,7,16,18	2,4,6,11,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,5,7,17,18	2,4,6,11,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,5,7,16	2,4,6,11,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,5,7,14,18	2,4,6,11,13,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,5,7,14,16,17	2,4,6,11,13,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,5,7,14	2,4,6,11,13,15	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,5,7,14,16,17,18	2,4,6,11,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,12	2,4,6,11	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,5,7,12,16,17,18	2,4,6,11,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,12,18	2,4,6,11,15,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,5,7,12,16,17	2,4,6,11,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,12,14,17,18	2,4,6,11,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,12,14,16	2,4,6,11	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,5,7,12,14,17	2,4,6,11,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,12,14,16,18	2,4,6,11,15,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,5,7,12,18	2,4,6,11,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,5,7,12,16,17	2,4,6,11,13,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,5,7,12	2,4,6,11,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,5,7,12,16,17,18	2,4,6,11,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,12,14,17	2,4,6,11,13,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,5,7,12,14,16,18	2,4,6,11,13,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,12,14,17,18	2,4,6,11,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,5,7,12,14,16	2,4,6,11,13,15	$2^{-28.5}$

Table 0.1779 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,5,7,10,18	2,4,6,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,5,7,10,16,17	2,4,6,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,5,7,10	2,4,6,15	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,5,7,10,16,17,18	2,4,6,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,5,7,10,14,17	2,4,6,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,5,7,10,14,16,18	2,4,6,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,5,7,10,14,17,18	2,4,6,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,5,7,10,14,16	2,4,6,15	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,5,7,10	2,4,6,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,5,7,10,16,17,18	2,4,6,13,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,5,7,10,18	2,4,6,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,5,7,10,16,17	2,4,6,13,15,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,5,7,10,14,17,18	2,4,6,13,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,5,7,10,14,16	2,4,6,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,5,7,10,14,17	2,4,6,13,15,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,5,7,10,14,16,18	2,4,6,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,5,7,10,12,17	2,4,6,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,5,7,10,12,16,18	2,4,6,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,5,7,10,12,17,18	2,4,6,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,5,7,10,12,16	2,4,6,15	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,5,7,10,12,14,18	2,4,6,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,5,7,10,12,14,16,17	2,4,6,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,5,7,10,12,14	2,4,6,15	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,5,7,10,12,14,16,17,18	2,4,6,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,5,7,10,12,17,18	2,4,6,13,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,5,7,10,12,16	2,4,6,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,5,7,10,12,17	2,4,6,13,15,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,5,7,10,12,16,18	2,4,6,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,7,10,12,14	2,4,6,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,5,7,10,12,14,16,17,18	2,4,6,13,17,18	2^{-34}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,5,7,10,12,14,18	2,4,6,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,5,7,10,12,14,16,17	2,4,6,13,15,17	2^{-34}

Table 0.1780 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,5,7,10	2,4,6,11	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,5,7,10,16,17,18	2,4,6,11,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,5,7,10,18	2,4,6,11,15,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,5,7,10,16,17	2,4,6,11,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,10,14,17,18	2,4,6,11,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,10,14,16	2,4,6,11	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,10,14,17	2,4,6,11,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,10,14,16,18	2,4,6,11,15,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,5,7,10,18	2,4,6,11,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,10,14,16,18	2,4,6,11,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,5,7,10,16,17	2,4,6,11,13,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,5,7,10	2,4,6,11,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,5,7,10,16,17,18	2,4,6,11,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,5,7,10,14,17	2,4,6,11,13,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,7,10,14,16,18	2,4,6,11,13,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,5,7,10,14,17,18	2,4,6,11,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,7,10,14,16	2,4,6,11,13,15	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,10,12,17,18	2,4,6,11,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,5,7,10,12,16	2,4,6,11	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,10,12,17	2,4,6,11,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,5,7,10,12,16,18	2,4,6,11,15,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,5,7,10,12,14	2,4,6,11	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,5,7,10,12,14,16,17,18	2,4,6,11,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,5,7,10,12,14,18	2,4,6,11,15,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,5,7,10,12,14,16,17	2,4,6,11,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,10,12,17	2,4,6,11,13,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,5,7,10,12,16,18	2,4,6,11,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,10,12,17,18	2,4,6,11,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,5,7,10,12,16	2,4,6,11,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,5,7,10,12,14,18	2,4,6,11,13,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,5,7,10,12,14,16,17	2,4,6,11,13,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,5,7,10,12,14	2,4,6,11,13,15	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,5,7,10,12,14,16,17,18	2,4,6,11,13,15,17,18	2^{-23}

Table 0.1781 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,5,7,17,18	2,4,6,9,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,5,7,16	2,4,6,9	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,5,7,17	2,4,6,9,15,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,5,7,16,18	2,4,6,9,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,5,7,14	2,4,6,9	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,5,7,14,16,17,18	2,4,6,9,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,5,7,14,18	2,4,6,9,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,5,7,14,16,17	2,4,6,9,15,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,5,7,17	2,4,6,9,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,5,7,16,18	2,4,6,9,13,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,5,7,17,18	2,4,6,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,5,7,16	2,4,6,9,13,15	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,5,7,14,18	2,4,6,9,13,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,5,7,14,16,17	2,4,6,9,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,5,7,14	2,4,6,9,13,15	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,5,7,14,16,17,18	2,4,6,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,5,7,12	2,4,6,9	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,5,7,12,16,17,18	2,4,6,9,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,5,7,12,18	2,4,6,9,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,5,7,12,16,17	2,4,6,9,15,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,5,7,12,14,17,18	2,4,6,9,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,5,7,12,14,16	2,4,6,9	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,5,7,12,14,17	2,4,6,9,15,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,5,7,12,14,16,18	2,4,6,9,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,5,7,12,18	2,4,6,9,13,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,5,7,12,16,17	2,4,6,9,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,5,7,12	2,4,6,9,13,15	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,5,7,12,16,17,18	2,4,6,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,5,7,12,14,17	2,4,6,9,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,5,7,12,14,16,18	2,4,6,9,13,18	2^{-34}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,5,7,12,14,17,18	2,4,6,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,5,7,12,14,16	2,4,6,9,13,15	2^{-34}

Table 0.1782 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,17	2,4,6,9,11,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,5,7,16,18	2,4,6,9,11,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,17,18	2,4,6,9,11,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,5,7,16	2,4,6,9,11,15	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,5,7,14,18	2,4,6,9,11,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,5,7,14,16,17	2,4,6,9,11,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,5,7,14	2,4,6,9,11,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,5,7,14,16,17,18	2,4,6,9,11,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,5,7,17,18	2,4,6,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,5,7,16	2,4,6,9,11,13	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,5,7,17	2,4,6,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,5,7,16,18	2,4,6,9,11,13,15,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,5,7,14	2,4,6,9,11,13	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,5,7,14,16,17,18	2,4,6,9,11,13,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,5,7,14,18	2,4,6,9,11,13,15,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,5,7,14,16,17	2,4,6,9,11,13,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,5,7,12,18	2,4,6,9,11,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,5,7,12,16,17	2,4,6,9,11,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,5,7,12	2,4,6,9,11,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,5,7,12,16,17,18	2,4,6,9,11,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,5,7,12,14,17	2,4,6,9,11,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,5,7,12,14,16,18	2,4,6,9,11,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,5,7,12,14,17,18	2,4,6,9,11,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,5,7,12,14,16	2,4,6,9,11,15	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,5,7,12	2,4,6,9,11,13	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,5,7,12,16,17,18	2,4,6,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,5,7,12,18	2,4,6,9,11,13,15,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,5,7,12,16,17	2,4,6,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,5,7,12,14,17,18	2,4,6,9,11,13,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,5,7,12,14,16	2,4,6,9,11,13	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,5,7,12,14,17	2,4,6,9,11,13,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,5,7,12,14,16,18	2,4,6,9,11,13,15,18	2^{-23}

Table 0.1783 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,5,7,10	2,4,6,9	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,5,7,10,16,17,18	2,4,6,9,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,5,7,10,18	2,4,6,9,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,5,7,10,16,17	2,4,6,9,15,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,5,7,10,14,17,18	2,4,6,9,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,5,7,10,14,16	2,4,6,9	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,5,7,10,14,17	2,4,6,9,15,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,5,7,10,14,16,18	2,4,6,9,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,5,7,10,18	2,4,6,9,13,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,5,7,10,16,17	2,4,6,9,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,5,7,10	2,4,6,9,13,15	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,5,7,10,16,17,18	2,4,6,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,5,7,10,14,17	2,4,6,9,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,5,7,10,14,16,18	2,4,6,9,13,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,5,7,10,14,17,18	2,4,6,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,5,7,10,14,16	2,4,6,9,13,15	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,5,7,10,12,17,18	2,4,6,9,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,5,7,10,12,16	2,4,6,9	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,5,7,10,12,17	2,4,6,9,15,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,5,7,10,12,16,18	2,4,6,9,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0)$	1,5,7,10,12,14	2,4,6,9	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,7,10,12,14,16,17,18	2,4,6,9,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,5,7,10,12,14,18	2,4,6,9,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,5,7,10,12,14,16,17	2,4,6,9,15,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,10,12,17	2,4,6,9,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,5,7,10,12,16,18	2,4,6,9,13,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,10,12,17,18	2,4,6,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,5,7,10,12,16	2,4,6,9,13,15	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,5,7,10,12,14,18	2,4,6,9,13,18	2^{-1}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,5,7,10,12,14,16,17	2,4,6,9,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,5,7,10,12,14	2,4,6,9,13,15	2^{-1}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,5,7,10,12,14,16,17,18	2,4,6,9,13,15,17,18	$2^{-17.5}$

Table 0.1784 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,5,7,10,18	2,4,6,9,11,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0)$	1,5,7,10,16,17	2,4,6,9,11,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,5,7,10	2,4,6,9,11,15	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,5,7,10,16,17,18	2,4,6,9,11,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,5,7,10,14,17	2,4,6,9,11,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,5,7,10,14,16,18	2,4,6,9,11,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,5,7,10,14,17,18	2,4,6,9,11,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,5,7,10,14,16	2,4,6,9,11,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,5,7,10	2,4,6,9,11,13	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,5,7,10,16,17,18	2,4,6,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,5,7,10,18	2,4,6,9,11,13,15,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,5,7,10,16,17	2,4,6,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,5,7,10,14,17,18	2,4,6,9,11,13,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,5,7,10,14,16	2,4,6,9,11,13	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1)$	1,5,7,10,14,17	2,4,6,9,11,13,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,5,7,10,14,16,18	2,4,6,9,11,13,15,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,10,12,17	2,4,6,9,11,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,10,12,16,18	2,4,6,9,11,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,10,12,17,18	2,4,6,9,11,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,10,12,16	2,4,6,9,11,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,10,12,14,18	2,4,6,9,11,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,5,7,10,12,14,16,17	2,4,6,9,11,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,10,12,14	2,4,6,9,11,15	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1)$	1,5,7,10,12,14,16,17,18	2,4,6,9,11,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,10,12,17,18	2,4,6,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,10,12,16	2,4,6,9,11,13	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,10,12,17	2,4,6,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,10,12,16,18	2,4,6,9,11,13,15,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,10,12,14	2,4,6,9,11,13	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,5,7,10,12,14,16,17,18	2,4,6,9,11,13,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,10,12,14,18	2,4,6,9,11,13,15,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,5,7,10,12,14,16,17	2,4,6,9,11,13,15,17	$2^{-28.5}$

Table 0.1785 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,5,7,18	2,4,6,8,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,5,7,16,17	2,4,6,8,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,5,7	2,4,6,8,15	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,5,7,16,17,18	2,4,6,8,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,5,7,14,17	2,4,6,8,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,5,7,14,16,18	2,4,6,8,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,5,7,14,17,18	2,4,6,8,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,5,7,14,16	2,4,6,8,15	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,5,7	2,4,6,8,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,5,7,16,17,18	2,4,6,8,13,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,5,7,18	2,4,6,8,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,5,7,16,17	2,4,6,8,13,15,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,5,7,14,17,18	2,4,6,8,13,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,5,7,14,16	2,4,6,8,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,5,7,14,17	2,4,6,8,13,15,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,5,7,14,16,18	2,4,6,8,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,5,7,12,17	2,4,6,8,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,5,7,12,16,18	2,4,6,8,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1)$	1,5,7,12,17,18	2,4,6,8,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,5,7,12,16	2,4,6,8,15	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,7,12,14,18	2,4,6,8,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,5,7,12,14,16,17	2,4,6,8,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,5,7,12,14	2,4,6,8,15	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,5,7,12,14,16,17,18	2,4,6,8,15,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,5,7,12,17,18	2,4,6,8,13,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,12,16	2,4,6,8,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,5,7,12,17	2,4,6,8,13,15,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,5,7,12,16,18	2,4,6,8,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,5,7,12,14	2,4,6,8,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,5,7,12,14,16,17,18	2,4,6,8,13,17,18	2^{-1}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,5,7,12,14,18	2,4,6,8,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,5,7,12,14,16,17	2,4,6,8,13,15,17	2^{-1}

Table 0.1786 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,5,7	2,4,6,8,11	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,5,7,16,17,18	2,4,6,8,11,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,5,7,18	2,4,6,8,11,15,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,5,7,16,17	2,4,6,8,11,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,5,7,14,17,18	2,4,6,8,11,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,5,7,14,16	2,4,6,8,11	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,5,7,14,17	2,4,6,8,11,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,5,7,14,16,18	2,4,6,8,11,15,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,5,7,18	2,4,6,8,11,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,5,7,16,17	2,4,6,8,11,13,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,5,7	2,4,6,8,11,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,5,7,16,17,18	2,4,6,8,11,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,5,7,14,17	2,4,6,8,11,13,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,5,7,14,16,18	2,4,6,8,11,13,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,5,7,14,17,18	2,4,6,8,11,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,5,7,14,16	2,4,6,8,11,13,15	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,5,7,12,17,18	2,4,6,8,11,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,5,7,12,16	2,4,6,8,11	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,5,7,12,17	2,4,6,8,11,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,5,7,12,16,18	2,4,6,8,11,15,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,7,12,14	2,4,6,8,11	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,5,7,12,14,16,17,18	2,4,6,8,11,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,5,7,12,14,18	2,4,6,8,11,15,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,5,7,12,14,16,17	2,4,6,8,11,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,5,7,12,17	2,4,6,8,11,13,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,5,7,12,16,18	2,4,6,8,11,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,5,7,12,17,18	2,4,6,8,11,13,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,5,7,12,16	2,4,6,8,11,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,5,7,12,14,18	2,4,6,8,11,13,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,5,7,12,14,16,17	2,4,6,8,11,13,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,5,7,12,14	2,4,6,8,11,13,15	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,5,7,12,14,16,17,18	2,4,6,8,11,13,15,17,18	2^{-12}

Table 0.1787 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,5,7,10,17	2,4,6,8,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,5,7,10,16,18	2,4,6,8,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,5,7,10,17,18	2,4,6,8,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,5,7,10,16	2,4,6,8,15	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,5,7,10,14,18	2,4,6,8,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,5,7,10,14,16,17	2,4,6,8,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,5,7,10,14	2,4,6,8,15	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,5,7,10,14,16,17,18	2,4,6,8,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,5,7,10,17,18	2,4,6,8,13,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,5,7,10,16	2,4,6,8,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,5,7,10,17	2,4,6,8,13,15,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,5,7,10,16,18	2,4,6,8,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,5,7,10,14	2,4,6,8,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,5,7,10,14,16,17,18	2,4,6,8,13,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,5,7,10,14,18	2,4,6,8,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,5,7,10,14,16,17	2,4,6,8,13,15,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,5,7,10,12,18	2,4,6,8,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,5,7,10,12,16,17	2,4,6,8,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,5,7,10,12	2,4,6,8,15	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,5,7,10,12,16,17,18	2,4,6,8,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,5,7,10,12,14,17	2,4,6,8,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,5,7,10,12,14,16,18	2,4,6,8,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,5,7,10,12,14,17,18	2,4,6,8,15,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,5,7,10,12,14,16	2,4,6,8,15	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,5,7,10,12	2,4,6,8,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,5,7,10,12,16,17,18	2,4,6,8,13,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,5,7,10,12,18	2,4,6,8,13,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,5,7,10,12,16,17	2,4,6,8,13,15,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,5,7,10,12,14,17,18	2,4,6,8,13,17,18	2^{-34}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,5,7,10,12,14,16	2,4,6,8,13	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,5,7,10,12,14,17	2,4,6,8,13,15,17	2^{-34}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,5,7,10,12,14,16,18	2,4,6,8,13,15,18	$2^{-17.5}$

Table 0.1788 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,5,7,10,17,18	2,4,6,8,11,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,10,16	2,4,6,8,11	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,5,7,10,17	2,4,6,8,11,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,10,16,18	2,4,6,8,11,15,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,5,7,10,14	2,4,6,8,11	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,5,7,10,14,16,17,18	2,4,6,8,11,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,5,7,10,14,18	2,4,6,8,11,15,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,5,7,10,14,16,17	2,4,6,8,11,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,5,7,10,17	2,4,6,8,11,13,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,5,7,10,16,18	2,4,6,8,11,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,5,7,10,17,18	2,4,6,8,11,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,5,7,10,16	2,4,6,8,11,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,5,7,10,14,18	2,4,6,8,11,13,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,5,7,10,14,16,17	2,4,6,8,11,13,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,5,7,10,14	2,4,6,8,11,13,15	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,5,7,10,14,16,17,18	2,4,6,8,11,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,5,7,10,12	2,4,6,8,11	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,5,7,10,12,16,17,18	2,4,6,8,11,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,5,7,10,12,18	2,4,6,8,11,15,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,5,7,10,12,16,17	2,4,6,8,11,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,5,7,10,12,14,17,18	2,4,6,8,11,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,5,7,10,12,14,16	2,4,6,8,11	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,5,7,10,12,14,17	2,4,6,8,11,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,5,7,10,12,14,16,18	2,4,6,8,11,15,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,5,7,10,12,18	2,4,6,8,11,13,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,5,7,10,12,16,17	2,4,6,8,11,13,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,5,7,10,12	2,4,6,8,11,13,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,5,7,10,12,16,17,18	2,4,6,8,11,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,5,7,10,12,14,17	2,4,6,8,11,13,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,5,7,10,12,14,16,18	2,4,6,8,11,13,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,5,7,10,12,14,17,18	2,4,6,8,11,13,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,5,7,10,12,14,16	2,4,6,8,11,13,15	$2^{-6.5}$

Table 0.1789 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,5,7	2,4,6,8,9	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,5,7,16,17,18	2,4,6,8,9,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,5,7,18	2,4,6,8,9,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,5,7,16,17	2,4,6,8,9,15,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,5,7,14,17,18	2,4,6,8,9,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,5,7,14,16	2,4,6,8,9	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,5,7,14,17	2,4,6,8,9,15,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,5,7,14,16,18	2,4,6,8,9,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,5,7,18	2,4,6,8,9,13,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,5,7,16,17	2,4,6,8,9,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,5,7	2,4,6,8,9,13,15	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,5,7,16,17,18	2,4,6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,5,7,14,17	2,4,6,8,9,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1)$	1,5,7,14,16,18	2,4,6,8,9,13,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,5,7,14,17,18	2,4,6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,14,16	2,4,6,8,9,13,15	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,12,17,18	2,4,6,8,9,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,5,7,12,16	2,4,6,8,9	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,12,17	2,4,6,8,9,15,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,5,7,12,16,18	2,4,6,8,9,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,5,7,12,14	2,4,6,8,9	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,12,14,16,17,18	2,4,6,8,9,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,5,7,12,14,18	2,4,6,8,9,15,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,12,14,16,17	2,4,6,8,9,15,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,12,17	2,4,6,8,9,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,12,16,18	2,4,6,8,9,13,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,12,17,18	2,4,6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,5,7,12,16	2,4,6,8,9,13,15	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,5,7,12,14,18	2,4,6,8,9,13,18	2^{-34}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,12,14,16,17	2,4,6,8,9,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,5,7,12,14	2,4,6,8,9,13,15	2^{-34}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,12,14,16,17,18	2,4,6,8,9,13,15,17,18	$2^{-17.5}$

Table 0.1790 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,5,7,18	2,4,6,8,9,11,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,5,7,16,17	2,4,6,8,9,11,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,5,7	2,4,6,8,9,11,15	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,5,7,16,17,18	2,4,6,8,9,11,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,14,17	2,4,6,8,9,11,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,14,16,18	2,4,6,8,9,11,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,5,7,14,17,18	2,4,6,8,9,11,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,5,7,14,16	2,4,6,8,9,11,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,5,7	2,4,6,8,9,11,13	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,5,7,16,17,18	2,4,6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,5,7,18	2,4,6,8,9,11,13,15,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,5,7,16,17	2,4,6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,7,14,17,18	2,4,6,8,9,11,13,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,5,7,14,16	2,4,6,8,9,11,13	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,5,7,14,17	2,4,6,8,9,11,13,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,5,7,14,16,18	2,4,6,8,9,11,13,15,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,5,7,12,17	2,4,6,8,9,11,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,12,16,18	2,4,6,8,9,11,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,5,7,12,17,18	2,4,6,8,9,11,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,5,7,12,16	2,4,6,8,9,11,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,5,7,12,14,18	2,4,6,8,9,11,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,5,7,12,14,16,17	2,4,6,8,9,11,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,5,7,12,14	2,4,6,8,9,11,15	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,5,7,12,14,16,17,18	2,4,6,8,9,11,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,5,7,12,17,18	2,4,6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,5,7,12,16	2,4,6,8,9,11,13	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,5,7,12,17	2,4,6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,5,7,12,16,18	2,4,6,8,9,11,13,15,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,5,7,12,14	2,4,6,8,9,11,13	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,5,7,12,14,16,17,18	2,4,6,8,9,11,13,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,5,7,12,14,18	2,4,6,8,9,11,13,15,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,5,7,12,14,16,17	2,4,6,8,9,11,13,15,17	$2^{-6.5}$

Table 0.1791 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,5,7,10,17,18	2,4,6,8,9,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,5,7,10,16	2,4,6,8,9	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,5,7,10,17	2,4,6,8,9,15,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,5,7,10,16,18	2,4,6,8,9,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,5,7,10,14	2,4,6,8,9	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,5,7,10,14,16,17,18	2,4,6,8,9,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,5,7,10,14,18	2,4,6,8,9,15,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,5,7,10,14,16,17	2,4,6,8,9,15,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,5,7,10,17	2,4,6,8,9,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,5,7,10,16,18	2,4,6,8,9,13,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,5,7,10,17,18	2,4,6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,5,7,10,16	2,4,6,8,9,13,15	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,7,10,14,18	2,4,6,8,9,13,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,5,7,10,14,16,17	2,4,6,8,9,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,5,7,10,14	2,4,6,8,9,13,15	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,5,7,10,14,16,17,18	2,4,6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,5,7,10,12	2,4,6,8,9	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,5,7,10,12,16,17,18	2,4,6,8,9,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,5,7,10,12,18	2,4,6,8,9,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,5,7,10,12,16,17	2,4,6,8,9,15,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,5,7,10,12,14,17,18	2,4,6,8,9,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,5,7,10,12,14,16	2,4,6,8,9	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,5,7,10,12,14,17	2,4,6,8,9,15,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,5,7,10,12,14,16,18	2,4,6,8,9,15,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,5,7,10,12,18	2,4,6,8,9,13,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,5,7,10,12,16,17	2,4,6,8,9,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,5,7,10,12	2,4,6,8,9,13,15	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,5,7,10,12,16,17,18	2,4,6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,5,7,10,12,14,17	2,4,6,8,9,13,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,5,7,10,12,14,16,18	2,4,6,8,9,13,18	2^{-1}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,5,7,10,12,14,17,18	2,4,6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,5,7,10,12,14,16	2,4,6,8,9,13,15	2^{-1}

Table 0.1792 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,5,7,10,17	2,4,6,8,9,11,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,5,7,10,16,18	2,4,6,8,9,11,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,5,7,10,17,18	2,4,6,8,9,11,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,5,7,10,16	2,4,6,8,9,11,15	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,5,7,10,14,18	2,4,6,8,9,11,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,5,7,10,14,16,17	2,4,6,8,9,11,17	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,5,7,10,14	2,4,6,8,9,11,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,5,7,10,14,16,17,18	2,4,6,8,9,11,15,17,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,5,7,10,17,18	2,4,6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,5,7,10,16	2,4,6,8,9,11,13	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,5,7,10,17	2,4,6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,5,7,10,16,18	2,4,6,8,9,11,13,15,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,5,7,10,14	2,4,6,8,9,11,13	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,5,7,10,14,16,17,18	2,4,6,8,9,11,13,17,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,5,7,10,14,18	2,4,6,8,9,11,13,15,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,5,7,10,14,16,17	2,4,6,8,9,11,13,15,17	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,5,7,10,12,18	2,4,6,8,9,11,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,10,12,16,17	2,4,6,8,9,11,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,5,7,10,12	2,4,6,8,9,11,15	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,5,7,10,12,16,17,18	2,4,6,8,9,11,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,10,12,14,17	2,4,6,8,9,11,17	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,5,7,10,12,14,16,18	2,4,6,8,9,11,18	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,5,7,10,12,14,17,18	2,4,6,8,9,11,15,17,18	2^{-23}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,5,7,10,12,14,16	2,4,6,8,9,11,15	$2^{-6.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,5,7,10,12	2,4,6,8,9,11,13	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,5,7,10,12,16,17,18	2,4,6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,5,7,10,12,18	2,4,6,8,9,11,13,15,18	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,5,7,10,12,16,17	2,4,6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,5,7,10,12,14,17,18	2,4,6,8,9,11,13,17,18	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,5,7,10,12,14,16	2,4,6,8,9,11,13	2^{-12}
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,5,7,10,12,14,17	2,4,6,8,9,11,13,15,17	$2^{-28.5}$
$(1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,5,7,10,12,14,16,18	2,4,6,8,9,11,13,15,18	2^{-12}

Table 0.1793 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,17,18	2,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,16	2	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,17	2,15,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,16,18	2,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,14	2	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,14,16,17,18	2,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,14,18	2,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,14,16,17	2,15,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,17	2,13,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,16,18	2,13,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,17,18	2,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,16	2,13,15	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,14,18	2,13,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,14,16,17	2,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,14	2,13,15	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,14,16,17,18	2,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,12	2	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,12,16,17,18	2,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,12,18	2,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,12,16,17	2,15,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,12,14,17,18	2,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,12,14,16	2	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,12,14,17	2,15,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,12,14,16,18	2,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,12,18	2,13,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,12,16,17	2,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,12	2,13,15	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,12,16,17,18	2,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,12,14,17	2,13,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,12,14,16,18	2,13,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,12,14,17,18	2,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,12,14,16	2,13,15	2^{-12}

Table 0.1794 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,17	2,11,17	2^{-1}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,16,18	2,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,17,18	2,11,15,17,18	2^{-1}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,16	2,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,14,18	2,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,14,16,17	2,11,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,14	2,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,14,16,17,18	2,11,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,17,18	2,11,13,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,16	2,11,13	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,17	2,11,13,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,16,18	2,11,13,15,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,14	2,11,13	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,14,16,17,18	2,11,13,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,14,18	2,11,13,15,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,14,16,17	2,11,13,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,12,18	2,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,12,16,17	2,11,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,12	2,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,12,16,17,18	2,11,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,12,14,17	2,11,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,12,14,16,18	2,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,12,14,17,18	2,11,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,12,14,16	2,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,12	2,11,13	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,12,16,17,18	2,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,12,18	2,11,13,15,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,12,16,17	2,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,12,14,17,18	2,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,12,14,16	2,11,13	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,12,14,17	2,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,12,14,16,18	2,11,13,15,18	2^{-23}

Table 0.1795 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,10	2	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,10,16,17,18	2,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,10,18	2,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,10,16,17	2,15,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,10,14,17,18	2,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,10,14,16	2	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,10,14,17	2,15,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,10,14,16,18	2,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,10,18	2,13,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,10,16,17	2,13,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,10	2,13,15	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,10,16,17,18	2,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,10,14,17	2,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,10,14,16,18	2,13,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,10,14,17,18	2,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,10,14,16	2,13,15	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,10,12,17,18	2,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,10,12,16	2	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,10,12,17	2,15,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,10,12,16,18	2,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,10,12,14	2	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,10,12,14,16,17,18	2,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,10,12,14,18	2,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,10,12,14,16,17	2,15,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,10,12,17	2,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,10,12,16,18	2,13,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,10,12,17,18	2,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,10,12,16	2,13,15	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,10,12,14,18	2,13,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,10,12,14,16,17	2,13,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,10,12,14	2,13,15	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,10,12,14,16,17,18	2,13,15,17,18	$2^{-28.5}$

Table 0.1796 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,10,18	2,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,10,16,17	2,11,17	2^{-34}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,10	2,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,10,16,17,18	2,11,15,17,18	2^{-34}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,10,14,17	2,11,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,10,14,16,18	2,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,10,14,17,18	2,11,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,10,14,16	2,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,10	2,11,13	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,10,16,17,18	2,11,13,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,10,18	2,11,13,15,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,10,16,17	2,11,13,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,10,14,17,18	2,11,13,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,10,14,16	2,11,13	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,10,14,17	2,11,13,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,10,14,16,18	2,11,13,15,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,10,12,17	2,11,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,10,12,16,18	2,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,10,12,17,18	2,11,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,10,12,16	2,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,10,12,14,18	2,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,10,12,14,16,17	2,11,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,10,12,14	2,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,10,12,14,16,17,18	2,11,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,10,12,17,18	2,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,10,12,16	2,11,13	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,10,12,17	2,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,10,12,16,18	2,11,13,15,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,10,12,14	2,11,13	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,10,12,14,16,17,18	2,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,10,12,14,18	2,11,13,15,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,10,12,14,16,17	2,11,13,15,17	$2^{-17.5}$

Table 0.1797 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,17	2,9,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,16,18	2,9,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,17,18	2,9,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,16	2,9,15	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,14,18	2,9,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,14,16,17	2,9,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,14	2,9,15	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,14,16,17,18	2,9,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,17,18	2,9,13,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,16	2,9,13	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,17	2,9,13,15,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1)$	1,3,16,18	2,9,13,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,14	2,9,13	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,14,16,17,18	2,9,13,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,14,18	2,9,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,14,16,17	2,9,13,15,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,12,18	2,9,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,12,16,17	2,9,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,12	2,9,15	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,12,16,17,18	2,9,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,12,14,17	2,9,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,12,14,16,18	2,9,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,12,14,17,18	2,9,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,12,14,16	2,9,15	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,12	2,9,13	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,12,16,17,18	2,9,13,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,12,18	2,9,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,12,16,17	2,9,13,15,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,12,14,17,18	2,9,13,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,12,14,16	2,9,13	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,12,14,17	2,9,13,15,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,12,14,16,18	2,9,13,15,18	$2^{-28.5}$

Table 0.1798 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,17,18	2,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,16	2,9,11	2^{-34}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,17	2,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,16,18	2,9,11,15,18	2^{-34}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,14	2,9,11	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,14,16,17,18	2,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,14,18	2,9,11,15,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,14,16,17	2,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,17	2,9,11,13,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,16,18	2,9,11,13,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,17,18	2,9,11,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,16	2,9,11,13,15	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,14,18	2,9,11,13,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,14,16,17	2,9,11,13,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,14	2,9,11,13,15	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,14,16,17,18	2,9,11,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,12	2,9,11	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,12,16,17,18	2,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,12,18	2,9,11,15,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,12,16,17	2,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,12,14,17,18	2,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,12,14,16	2,9,11	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,12,14,17	2,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,12,14,16,18	2,9,11,15,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,12,18	2,9,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,12,16,17	2,9,11,13,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,12	2,9,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,12,16,17,18	2,9,11,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,12,14,17	2,9,11,13,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,12,14,16,18	2,9,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,12,14,17,18	2,9,11,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,12,14,16	2,9,11,13,15	$2^{-17.5}$

Table 0.1799 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,10,18	2,9,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,10,16,17	2,9,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,10	2,9,15	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,10,16,17,18	2,9,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,10,14,17	2,9,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,10,14,16,18	2,9,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,10,14,17,18	2,9,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,10,14,16	2,9,15	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,10	2,9,13	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,10,16,17,18	2,9,13,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,10,18	2,9,13,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,10,16,17	2,9,13,15,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,10,14,17,18	2,9,13,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,10,14,16	2,9,13	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,10,14,17	2,9,13,15,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,10,14,16,18	2,9,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,10,12,17	2,9,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,10,12,16,18	2,9,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,10,12,17,18	2,9,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,10,12,16	2,9,15	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,10,12,14,18	2,9,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,10,12,14,16,17	2,9,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,10,12,14	2,9,15	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,10,12,14,16,17,18	2,9,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,10,12,17,18	2,9,13,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,10,12,16	2,9,13	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,10,12,17	2,9,13,15,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,10,12,16,18	2,9,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,10,12,14	2,9,13	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,10,12,14,16,17,18	2,9,13,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,10,12,14,18	2,9,13,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,10,12,14,16,17	2,9,13,15,17	2^{-12}

Table 0.1800 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,10	2,9,11	2^{-1}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,10,16,17,18	2,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,10,18	2,9,11,15,18	2^{-1}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,10,16,17	2,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,10,14,17,18	2,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,10,14,16	2,9,11	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,10,14,17	2,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,10,14,16,18	2,9,11,15,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,10,18	2,9,11,13,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,10,16,17	2,9,11,13,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,10	2,9,11,13,15	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,10,16,17,18	2,9,11,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,10,14,17	2,9,11,13,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,10,14,16,18	2,9,11,13,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,10,14,17,18	2,9,11,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,10,14,16	2,9,11,13,15	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,10,12,17,18	2,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,10,12,16	2,9,11	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,10,12,17	2,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,10,12,16,18	2,9,11,15,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,10,12,14	2,9,11	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,10,12,14,16,17,18	2,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,10,12,14,18	2,9,11,15,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,10,12,14,16,17	2,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,10,12,17	2,9,11,13,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,10,12,16,18	2,9,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,10,12,17,18	2,9,11,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,10,12,16	2,9,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,10,12,14,18	2,9,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,10,12,14,16,17	2,9,11,13,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,10,12,14	2,9,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,10,12,14,16,17,18	2,9,11,13,15,17,18	2^{-23}

Table 0.1801 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3	2,8	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,16,17,18	2,8,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,18	2,8,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,16,17	2,8,15,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,14,17,18	2,8,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,14,16	2,8	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,14,17	2,8,15,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,14,16,18	2,8,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,18	2,8,13,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,16,17	2,8,13,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3	2,8,13,15	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,16,17,18	2,8,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,14,17	2,8,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,14,16,18	2,8,13,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,14,17,18	2,8,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,14,16	2,8,13,15	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,12,17,18	2,8,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,12,16	2,8	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,12,17	2,8,15,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,12,16,18	2,8,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,12,14	2,8	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,12,14,16,17,18	2,8,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,12,14,18	2,8,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,12,14,16,17	2,8,15,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,12,17	2,8,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,12,16,18	2,8,13,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,12,17,18	2,8,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,12,16	2,8,13,15	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,12,14,18	2,8,13,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,12,14,16,17	2,8,13,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,12,14	2,8,13,15	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,12,14,16,17,18	2,8,13,15,17,18	$2^{-6.5}$

Table 0.1802 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,18	2,8,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,16,17	2,8,11,17	2^{-1}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3	2,8,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,16,17,18	2,8,11,15,17,18	2^{-1}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,14,17	2,8,11,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,14,16,18	2,8,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,14,17,18	2,8,11,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,14,16	2,8,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3	2,8,11,13	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,16,17,18	2,8,11,13,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,18	2,8,11,13,15,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,16,17	2,8,11,13,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,14,17,18	2,8,11,13,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,14,16	2,8,11,13	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,14,17	2,8,11,13,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,14,16,18	2,8,11,13,15,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,12,17	2,8,11,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,12,16,18	2,8,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,12,17,18	2,8,11,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,12,16	2,8,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,12,14,18	2,8,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,12,14,16,17	2,8,11,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,12,14	2,8,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,12,14,16,17,18	2,8,11,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,12,17,18	2,8,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,12,16	2,8,11,13	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,12,17	2,8,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,12,16,18	2,8,11,13,15,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,12,14	2,8,11,13	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,12,14,16,17,18	2,8,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,12,14,18	2,8,11,13,15,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,12,14,16,17	2,8,11,13,15,17	$2^{-17.5}$

Table 0.1803 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,10,17,18	2,8,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,10,16	2,8	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,10,17	2,8,15,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,10,16,18	2,8,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,10,14	2,8	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,10,14,16,17,18	2,8,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,10,14,18	2,8,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,10,14,16,17	2,8,15,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,10,17	2,8,13,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,10,16,18	2,8,13,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,10,17,18	2,8,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,10,16	2,8,13,15	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,10,14,18	2,8,13,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,10,14,16,17	2,8,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,10,14	2,8,13,15	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,10,14,16,17,18	2,8,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,10,12	2,8	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,10,12,16,17,18	2,8,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,10,12,18	2,8,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0)$	1,3,10,12,16,17	2,8,15,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,10,12,14,17,18	2,8,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,10,12,14,16	2,8	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,10,12,14,17	2,8,15,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,10,12,14,16,18	2,8,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,10,12,18	2,8,13,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,10,12,16,17	2,8,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,10,12	2,8,13,15	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,10,12,16,17,18	2,8,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,10,12,14,17	2,8,13,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,10,12,14,16,18	2,8,13,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,10,12,14,17,18	2,8,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,10,12,14,16	2,8,13,15	2^{-23}

Table 0.1804 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,10,17	2,8,11,17	2^{-34}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,10,16,18	2,8,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,10,17,18	2,8,11,15,17,18	2^{-34}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,10,16	2,8,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,10,14,18	2,8,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,10,14,16,17	2,8,11,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,10,14	2,8,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,10,14,16,17,18	2,8,11,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,10,17,18	2,8,11,13,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,10,16	2,8,11,13	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,10,17	2,8,11,13,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,10,16,18	2,8,11,13,15,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,10,14	2,8,11,13	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,10,14,16,17,18	2,8,11,13,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,10,14,18	2,8,11,13,15,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,10,14,16,17	2,8,11,13,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,10,12,18	2,8,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,10,12,16,17	2,8,11,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,10,12	2,8,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,10,12,16,17,18	2,8,11,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,10,12,14,17	2,8,11,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,10,12,14,16,18	2,8,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,10,12,14,17,18	2,8,11,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,10,12,14,16	2,8,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,10,12	2,8,11,13	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,10,12,16,17,18	2,8,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,10,12,18	2,8,11,13,15,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,10,12,16,17	2,8,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,10,12,14,17,18	2,8,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,10,12,14,16	2,8,11,13	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,10,12,14,17	2,8,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,10,12,14,16,18	2,8,11,13,15,18	2^{-12}

Table 0.1805 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,18	2,8,9,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,16,17	2,8,9,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3	2,8,9,15	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,16,17,18	2,8,9,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,14,17	2,8,9,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,14,16,18	2,8,9,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,14,17,18	2,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,14,16	2,8,9,15	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3	2,8,9,13	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,16,17,18	2,8,9,13,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,18	2,8,9,13,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,16,17	2,8,9,13,15,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,14,17,18	2,8,9,13,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,14,16	2,8,9,13	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,14,17	2,8,9,13,15,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,14,16,18	2,8,9,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,12,17	2,8,9,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,12,16,18	2,8,9,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,12,17,18	2,8,9,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,12,16	2,8,9,15	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,12,14,18	2,8,9,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,12,14,16,17	2,8,9,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,12,14	2,8,9,15	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,12,14,16,17,18	2,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,12,17,18	2,8,9,13,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,12,16	2,8,9,13	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,12,17	2,8,9,13,15,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,12,16,18	2,8,9,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,12,14	2,8,9,13	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,12,14,16,17,18	2,8,9,13,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,12,14,18	2,8,9,13,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,12,14,16,17	2,8,9,13,15,17	2^{-23}

Table 0.1806 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3	2,8,9,11	2^{-34}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,16,17,18	2,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,18	2,8,9,11,15,18	2^{-34}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,16,17	2,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,14,17,18	2,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,14,16	2,8,9,11	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,14,17	2,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,14,16,18	2,8,9,11,15,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,18	2,8,9,11,13,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,16,17	2,8,9,11,13,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3	2,8,9,11,13,15	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,16,17,18	2,8,9,11,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,14,17	2,8,9,11,13,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,14,16,18	2,8,9,11,13,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,14,17,18	2,8,9,11,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,14,16	2,8,9,11,13,15	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,12,17,18	2,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,12,16	2,8,9,11	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,12,17	2,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,12,16,18	2,8,9,11,15,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1)$	1,3,12,14	2,8,9,11	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,12,14,16,17,18	2,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,12,14,18	2,8,9,11,15,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,12,14,16,17	2,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,12,17	2,8,9,11,13,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,12,16,18	2,8,9,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,12,17,18	2,8,9,11,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,12,16	2,8,9,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,12,14,18	2,8,9,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,12,14,16,17	2,8,9,11,13,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,12,14	2,8,9,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,12,14,16,17,18	2,8,9,11,13,15,17,18	2^{-12}

Table 0.1807 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,10,17	2,8,9,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,10,16,18	2,8,9,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,10,17,18	2,8,9,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,10,16	2,8,9,15	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,10,14,18	2,8,9,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,10,14,16,17	2,8,9,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,10,14	2,8,9,15	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,10,14,16,17,18	2,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,10,17,18	2,8,9,13,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,10,16	2,8,9,13	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,10,17	2,8,9,13,15,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,10,16,18	2,8,9,13,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,10,14	2,8,9,13	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,10,14,16,17,18	2,8,9,13,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,10,14,18	2,8,9,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,10,14,16,17	2,8,9,13,15,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,10,12,18	2,8,9,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,10,12,16,17	2,8,9,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,10,12	2,8,9,15	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,10,12,16,17,18	2,8,9,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,10,12,14,17	2,8,9,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,10,12,14,16,18	2,8,9,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,10,12,14,17,18	2,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,10,12,14,16	2,8,9,15	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,10,12	2,8,9,13	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,10,12,16,17,18	2,8,9,13,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,10,12,18	2,8,9,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,10,12,16,17	2,8,9,13,15,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,10,12,14,17,18	2,8,9,13,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,10,12,14,16	2,8,9,13	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,10,12,14,17	2,8,9,13,15,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,10,12,14,16,18	2,8,9,13,15,18	$2^{-6.5}$

Table 0.1808 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,10,17,18	2,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,10,16	2,8,9,11	2^{-1}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,10,17	2,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,10,16,18	2,8,9,11,15,18	2^{-1}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,10,14	2,8,9,11	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,10,14,16,17,18	2,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,10,14,18	2,8,9,11,15,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,10,14,16,17	2,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,10,17	2,8,9,11,13,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,10,16,18	2,8,9,11,13,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,10,17,18	2,8,9,11,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,10,16	2,8,9,11,13,15	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,10,14,18	2,8,9,11,13,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,10,14,16,17	2,8,9,11,13,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,10,14	2,8,9,11,13,15	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,10,14,16,17,18	2,8,9,11,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,10,12	2,8,9,11	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,10,12,16,17,18	2,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,10,12,18	2,8,9,11,15,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,10,12,16,17	2,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,10,12,14,17,18	2,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,10,12,14,16	2,8,9,11	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,10,12,14,17	2,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,10,12,14,16,18	2,8,9,11,15,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,10,12,18	2,8,9,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,10,12,16,17	2,8,9,11,13,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,10,12	2,8,9,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,10,12,16,17,18	2,8,9,11,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,10,12,14,17	2,8,9,11,13,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,10,12,14,16,18	2,8,9,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,10,12,14,17,18	2,8,9,11,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,10,12,14,16	2,8,9,11,13,15	$2^{-17.5}$

Table 0.1809 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,7,17	2,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,7,16,18	2,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,7,17,18	2,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,7,16	2,15	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,7,14,18	2,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,7,14,16,17	2,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,7,14	2,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,7,14,16,17,18	2,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,7,17,18	2,13,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,7,16	2,13	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,7,17	2,13,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,7,16,18	2,13,15,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,7,14	2,13	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,7,14,16,17,18	2,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,7,14,18	2,13,15,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,7,14,16,17	2,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,7,12,18	2,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,7,12,16,17	2,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,7,12	2,15	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,7,12,16,17,18	2,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,7,12,14,17	2,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,7,12,14,16,18	2,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,7,12,14,17,18	2,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,7,12,14,16	2,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,7,12	2,13	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,7,12,16,17,18	2,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,7,12,18	2,13,15,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,7,12,16,17	2,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,7,12,14,17,18	2,13,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,7,12,14,16	2,13	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,7,12,14,17	2,13,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,7,12,14,16,18	2,13,15,18	2^{-12}

Table 0.1810 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,7,17,18	2,11,17,18	2^{-1}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,7,16	2,11	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,7,17	2,11,15,17	2^{-1}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,7,16,18	2,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,7,14	2,11	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,7,14,16,17,18	2,11,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,7,14,18	2,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1)$	1,3,7,14,16,17	2,11,15,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,17	2,11,13,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,7,16,18	2,11,13,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,17,18	2,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,7,16	2,11,13,15	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,7,14,18	2,11,13,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,14,16,17	2,11,13,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,7,14	2,11,13,15	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,14,16,17,18	2,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,7,12	2,11	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1)$	1,3,7,12,16,17,18	2,11,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,7,12,18	2,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,7,12,16,17	2,11,15,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,7,12,14,17,18	2,11,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,7,12,14,16	2,11	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,7,12,14,17	2,11,15,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,7,12,14,16,18	2,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,7,12,18	2,11,13,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,7,12,16,17	2,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,7,12	2,11,13,15	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,7,12,16,17,18	2,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,7,12,14,17	2,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,7,12,14,16,18	2,11,13,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,7,12,14,17,18	2,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,7,12,14,16	2,11,13,15	2^{-23}

Table 0.1811 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,7,10,18	2,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,7,10,16,17	2,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,7,10	2,15	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,7,10,16,17,18	2,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,7,10,14,17	2,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,7,10,14,16,18	2,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,7,10,14,17,18	2,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,7,10,14,16	2,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,7,10	2,13	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,7,10,16,17,18	2,13,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,7,10,18	2,13,15,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,7,10,16,17	2,13,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,7,10,14,17,18	2,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,7,10,14,16	2,13	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,7,10,14,17	2,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,7,10,14,16,18	2,13,15,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,7,10,12,17	2,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,7,10,12,16,18	2,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1)$	1,3,7,10,12,17,18	2,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,7,10,12,16	2,15	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,7,10,12,14,18	2,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,7,10,12,14,16,17	2,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,7,10,12,14	2,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,7,10,12,14,16,17,18	2,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,7,10,12,17,18	2,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,7,10,12,16	2,13	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,7,10,12,17	2,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,7,10,12,16,18	2,13,15,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,7,10,12,14	2,13	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,7,10,12,14,16,17,18	2,13,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,7,10,12,14,18	2,13,15,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,7,10,12,14,16,17	2,13,15,17	$2^{-28.5}$

Table 0.1812 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,7,10	2,11	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,7,10,16,17,18	2,11,17,18	2^{-34}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,7,10,18	2,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,7,10,16,17	2,11,15,17	2^{-34}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,7,10,14,17,18	2,11,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,7,10,14,16	2,11	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,7,10,14,17	2,11,15,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,7,10,14,16,18	2,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,7,10,18	2,11,13,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,7,10,16,17	2,11,13,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,7,10	2,11,13,15	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,7,10,16,17,18	2,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,7,10,14,17	2,11,13,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,7,10,14,16,18	2,11,13,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,7,10,14,17,18	2,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,7,10,14,16	2,11,13,15	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,7,10,12,17,18	2,11,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,7,10,12,16	2,11	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,7,10,12,17	2,11,15,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,7,10,12,16,18	2,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,7,10,12,14	2,11	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,7,10,12,14,16,17,18	2,11,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,7,10,12,14,18	2,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,7,10,12,14,16,17	2,11,15,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,7,10,12,17	2,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,7,10,12,16,18	2,11,13,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,7,10,12,17,18	2,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,7,10,12,16	2,11,13,15	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,7,10,12,14,18	2,11,13,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,7,10,12,14,16,17	2,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,7,10,12,14	2,11,13,15	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,7,10,12,14,16,17,18	2,11,13,15,17,18	$2^{-17.5}$

Table 0.1813 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,7,17,18	2,9,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,7,16	2,9	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,7,17	2,9,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,7,16,18	2,9,15,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,7,14	2,9	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,7,14,16,17,18	2,9,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,7,14,18	2,9,15,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,7,14,16,17	2,9,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,17	2,9,13,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,7,16,18	2,9,13,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,17,18	2,9,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,7,16	2,9,13,15	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,7,14,18	2,9,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,7,14,16,17	2,9,13,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,7,14	2,9,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,7,14,16,17,18	2,9,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,7,12	2,9	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,7,12,16,17,18	2,9,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,7,12,18	2,9,15,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,7,12,16,17	2,9,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,7,12,14,17,18	2,9,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,7,12,14,16	2,9	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,7,12,14,17	2,9,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,7,12,14,16,18	2,9,15,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,7,12,18	2,9,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,7,12,16,17	2,9,13,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,7,12	2,9,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,7,12,16,17,18	2,9,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,7,12,14,17	2,9,13,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,7,12,14,16,18	2,9,13,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,7,12,14,17,18	2,9,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,7,12,14,16	2,9,13,15	$2^{-28.5}$

Table 0.1814 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,7,17	2,9,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,7,16,18	2,9,11,18	2^{-34}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,7,17,18	2,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,7,16	2,9,11,15	2^{-34}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,7,14,18	2,9,11,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,7,14,16,17	2,9,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,7,14	2,9,11,15	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,7,14,16,17,18	2,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,7,17,18	2,9,11,13,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,7,16	2,9,11,13	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,7,17	2,9,11,13,15,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,7,16,18	2,9,11,13,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,7,14	2,9,11,13	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,7,14,16,17,18	2,9,11,13,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,7,14,18	2,9,11,13,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,7,14,16,17	2,9,11,13,15,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,7,12,18	2,9,11,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,7,12,16,17	2,9,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,7,12	2,9,11,15	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,7,12,16,17,18	2,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,7,12,14,17	2,9,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,7,12,14,16,18	2,9,11,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,7,12,14,17,18	2,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,7,12,14,16	2,9,11,15	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,7,12	2,9,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,7,12,16,17,18	2,9,11,13,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,7,12,18	2,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,7,12,16,17	2,9,11,13,15,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,7,12,14,17,18	2,9,11,13,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,7,12,14,16	2,9,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,7,12,14,17	2,9,11,13,15,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,7,12,14,16,18	2,9,11,13,15,18	$2^{-17.5}$

Table 0.1815 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,7,10	2,9	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,7,10,16,17,18	2,9,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,7,10,18	2,9,15,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,7,10,16,17	2,9,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,7,10,14,17,18	2,9,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,7,10,14,16	2,9	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,7,10,14,17	2,9,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,7,10,14,16,18	2,9,15,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,7,10,18	2,9,13,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,7,10,16,17	2,9,13,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,7,10	2,9,13,15	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,7,10,16,17,18	2,9,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,7,10,14,17	2,9,13,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,7,10,14,16,18	2,9,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,7,10,14,17,18	2,9,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,7,10,14,16	2,9,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,7,10,12,17,18	2,9,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,7,10,12,16	2,9	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,7,10,12,17	2,9,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,7,10,12,16,18	2,9,15,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,7,10,12,14	2,9	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,7,10,12,14,16,17,18	2,9,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,7,10,12,14,18	2,9,15,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,7,10,12,14,16,17	2,9,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1)$	1,3,7,10,12,17	2,9,13,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,7,10,12,16,18	2,9,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,7,10,12,17,18	2,9,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,7,10,12,16	2,9,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,7,10,12,14,18	2,9,13,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,7,10,12,14,16,17	2,9,13,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,7,10,12,14	2,9,13,15	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,7,10,12,14,16,17,18	2,9,13,15,17,18	2^{-12}

Table 0.1816 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,7,10,18	2,9,11,18	2^{-1}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,7,10,16,17	2,9,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,7,10	2,9,11,15	2^{-1}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,7,10,16,17,18	2,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,7,10,14,17	2,9,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,7,10,14,16,18	2,9,11,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,7,10,14,17,18	2,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,7,10,14,16	2,9,11,15	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,7,10	2,9,11,13	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,7,10,16,17,18	2,9,11,13,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,7,10,18	2,9,11,13,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,7,10,16,17	2,9,11,13,15,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,7,10,14,17,18	2,9,11,13,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,7,10,14,16	2,9,11,13	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,7,10,14,17	2,9,11,13,15,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,7,10,14,16,18	2,9,11,13,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1)$	1,3,7,10,12,17	2,9,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,7,10,12,16,18	2,9,11,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,7,10,12,17,18	2,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,7,10,12,16	2,9,11,15	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,7,10,12,14,18	2,9,11,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,7,10,12,14,16,17	2,9,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,7,10,12,14	2,9,11,15	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,7,10,12,14,16,17,18	2,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,7,10,12,17,18	2,9,11,13,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,7,10,12,16	2,9,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,7,10,12,17	2,9,11,13,15,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,7,10,12,16,18	2,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,7,10,12,14	2,9,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,7,10,12,14,16,17,18	2,9,11,13,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,7,10,12,14,18	2,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,7,10,12,14,16,17	2,9,11,13,15,17	2^{-23}

Table 0.1817 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,7,18	2,8,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,7,16,17	2,8,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,7	2,8,15	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,7,16,17,18	2,8,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,7,14,17	2,8,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,7,14,16,18	2,8,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,7,14,17,18	2,8,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,7,14,16	2,8,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,7	2,8,13	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,7,16,17,18	2,8,13,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,7,18	2,8,13,15,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,7,16,17	2,8,13,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,7,14,17,18	2,8,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,7,14,16	2,8,13	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,7,14,17	2,8,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,7,14,16,18	2,8,13,15,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,7,12,17	2,8,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,7,12,16,18	2,8,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,7,12,17,18	2,8,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,7,12,16	2,8,15	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,7,12,14,18	2,8,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,7,12,14,16,17	2,8,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,7,12,14	2,8,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,7,12,14,16,17,18	2,8,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,7,12,17,18	2,8,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,7,12,16	2,8,13	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,7,12,17	2,8,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,7,12,16,18	2,8,13,15,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,7,12,14	2,8,13	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,7,12,14,16,17,18	2,8,13,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,7,12,14,18	2,8,13,15,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,7,12,14,16,17	2,8,13,15,17	$2^{-6.5}$

Table 0.1818 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,7	2,8,11	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,7,16,17,18	2,8,11,17,18	2^{-1}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,7,18	2,8,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,7,16,17	2,8,11,15,17	2^{-1}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,7,14,17,18	2,8,11,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,7,14,16	2,8,11	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,7,14,17	2,8,11,15,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,7,14,16,18	2,8,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,7,18	2,8,11,13,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,7,16,17	2,8,11,13,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,7	2,8,11,13,15	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,7,16,17,18	2,8,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,7,14,17	2,8,11,13,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,7,14,16,18	2,8,11,13,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,7,14,17,18	2,8,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,7,14,16	2,8,11,13,15	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,7,12,17,18	2,8,11,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,7,12,16	2,8,11	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,7,12,17	2,8,11,15,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1)$	1,3,7,12,16,18	2,8,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,7,12,14	2,8,11	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,7,12,14,16,17,18	2,8,11,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,7,12,14,18	2,8,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,7,12,14,16,17	2,8,11,15,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,7,12,17	2,8,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,7,12,16,18	2,8,11,13,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,7,12,17,18	2,8,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,7,12,16	2,8,11,13,15	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,7,12,14,18	2,8,11,13,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,7,12,14,16,17	2,8,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,7,12,14	2,8,11,13,15	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,7,12,14,16,17,18	2,8,11,13,15,17,18	$2^{-17.5}$

Table 0.1819 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,7,10,17	2,8,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,7,10,16,18	2,8,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,7,10,17,18	2,8,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,7,10,16	2,8,15	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,7,10,14,18	2,8,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,7,10,14,16,17	2,8,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,7,10,14	2,8,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,7,10,14,16,17,18	2,8,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,7,10,17,18	2,8,13,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,10,16	2,8,13	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,7,10,17	2,8,13,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,10,16,18	2,8,13,15,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,7,10,14	2,8,13	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,7,10,14,16,17,18	2,8,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,7,10,14,18	2,8,13,15,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,7,10,14,16,17	2,8,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,7,10,12,18	2,8,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,7,10,12,16,17	2,8,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,7,10,12	2,8,15	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,7,10,12,16,17,18	2,8,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,7,10,12,14,17	2,8,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,7,10,12,14,16,18	2,8,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,7,10,12,14,17,18	2,8,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,7,10,12,14,16	2,8,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,7,10,12	2,8,13	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,7,10,12,16,17,18	2,8,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,7,10,12,18	2,8,13,15,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,7,10,12,16,17	2,8,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,7,10,12,14,17,18	2,8,13,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,7,10,12,14,16	2,8,13	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,7,10,12,14,17	2,8,13,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,7,10,12,14,16,18	2,8,13,15,18	2^{-23}

Table 0.1820 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,7,10,17,18	2,8,11,17,18	2^{-34}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,7,10,16	2,8,11	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,7,10,17	2,8,11,15,17	2^{-34}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,7,10,16,18	2,8,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,7,10,14	2,8,11	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,7,10,14,16,17,18	2,8,11,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,7,10,14,18	2,8,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,7,10,14,16,17	2,8,11,15,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,7,10,17	2,8,11,13,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,7,10,16,18	2,8,11,13,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,7,10,17,18	2,8,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,7,10,16	2,8,11,13,15	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,7,10,14,18	2,8,11,13,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,7,10,14,16,17	2,8,11,13,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,7,10,14	2,8,11,13,15	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,7,10,14,16,17,18	2,8,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,7,10,12	2,8,11	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,7,10,12,16,17,18	2,8,11,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,7,10,12,18	2,8,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,7,10,12,16,17	2,8,11,15,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,7,10,12,14,17,18	2,8,11,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,7,10,12,14,16	2,8,11	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,7,10,12,14,17	2,8,11,15,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,7,10,12,14,16,18	2,8,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,7,10,12,18	2,8,11,13,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,7,10,12,16,17	2,8,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,7,10,12	2,8,11,13,15	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,7,10,12,16,17,18	2,8,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,7,10,12,14,17	2,8,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,7,10,12,14,16,18	2,8,11,13,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,7,10,12,14,17,18	2,8,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,7,10,12,14,16	2,8,11,13,15	2^{-12}

Table 0.1821 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,7	2,8,9	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,7,16,17,18	2,8,9,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,7,18	2,8,9,15,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,7,16,17	2,8,9,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,7,14,17,18	2,8,9,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,7,14,16	2,8,9	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,7,14,17	2,8,9,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,7,14,16,18	2,8,9,15,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,7,18	2,8,9,13,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,7,16,17	2,8,9,13,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,7	2,8,9,13,15	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,7,16,17,18	2,8,9,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,7,14,17	2,8,9,13,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,7,14,16,18	2,8,9,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,7,14,17,18	2,8,9,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,7,14,16	2,8,9,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,7,12,17,18	2,8,9,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,7,12,16	2,8,9	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,7,12,17	2,8,9,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,7,12,16,18	2,8,9,15,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,7,12,14	2,8,9	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,7,12,14,16,17,18	2,8,9,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,7,12,14,18	2,8,9,15,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,7,12,14,16,17	2,8,9,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,7,12,17	2,8,9,13,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,7,12,16,18	2,8,9,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,7,12,17,18	2,8,9,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,7,12,16	2,8,9,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,7,12,14,18	2,8,9,13,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,7,12,14,16,17	2,8,9,13,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,7,12,14	2,8,9,13,15	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,7,12,14,16,17,18	2,8,9,13,15,17,18	2^{-23}

Table 0.1822 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,7,18	2,8,9,11,18	2^{-34}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,7,16,17	2,8,9,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,7	2,8,9,11,15	2^{-34}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,7,16,17,18	2,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,7,14,17	2,8,9,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,7,14,16,18	2,8,9,11,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,7,14,17,18	2,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,7,14,16	2,8,9,11,15	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,7	2,8,9,11,13	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,7,16,17,18	2,8,9,11,13,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,7,18	2,8,9,11,13,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,7,16,17	2,8,9,11,13,15,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,7,14,17,18	2,8,9,11,13,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,7,14,16	2,8,9,11,13	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,7,14,17	2,8,9,11,13,15,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,7,14,16,18	2,8,9,11,13,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,7,12,17	2,8,9,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,7,12,16,18	2,8,9,11,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,7,12,17,18	2,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,7,12,16	2,8,9,11,15	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,7,12,14,18	2,8,9,11,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,7,12,14,16,17	2,8,9,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,7,12,14	2,8,9,11,15	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,7,12,14,16,17,18	2,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,7,12,17,18	2,8,9,11,13,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,7,12,16	2,8,9,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,7,12,17	2,8,9,11,13,15,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,7,12,16,18	2,8,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,7,12,14	2,8,9,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,7,12,14,16,17,18	2,8,9,11,13,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,7,12,14,18	2,8,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,7,12,14,16,17	2,8,9,11,13,15,17	2^{-12}

Table 0.1823 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,7,10,17,18	2,8,9,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,7,10,16	2,8,9	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,7,10,17	2,8,9,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,7,10,16,18	2,8,9,15,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,7,10,14	2,8,9	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,7,10,14,16,17,18	2,8,9,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,7,10,14,18	2,8,9,15,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,7,10,14,16,17	2,8,9,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,7,10,17	2,8,9,13,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,7,10,16,18	2,8,9,13,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,7,10,17,18	2,8,9,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,7,10,16	2,8,9,13,15	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,7,10,14,18	2,8,9,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,7,10,14,16,17	2,8,9,13,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,7,10,14	2,8,9,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,7,10,14,16,17,18	2,8,9,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,7,10,12	2,8,9	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,7,10,12,16,17,18	2,8,9,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,7,10,12,18	2,8,9,15,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,7,10,12,16,17	2,8,9,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,7,10,12,14,17,18	2,8,9,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,7,10,12,14,16	2,8,9	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,7,10,12,14,17	2,8,9,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,7,10,12,14,16,18	2,8,9,15,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,7,10,12,18	2,8,9,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,7,10,12,16,17	2,8,9,13,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,7,10,12	2,8,9,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,7,10,12,16,17,18	2,8,9,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,7,10,12,14,17	2,8,9,13,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,7,10,12,14,16,18	2,8,9,13,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,7,10,12,14,17,18	2,8,9,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,7,10,12,14,16	2,8,9,13,15	$2^{-6.5}$

Table 0.1824 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,7,10,17	2,8,9,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,7,10,16,18	2,8,9,11,18	2^{-1}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,7,10,17,18	2,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,7,10,16	2,8,9,11,15	2^{-1}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,7,10,14,18	2,8,9,11,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,7,10,14,16,17	2,8,9,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,7,10,14	2,8,9,11,15	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,7,10,14,16,17,18	2,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,7,10,17,18	2,8,9,11,13,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,7,10,16	2,8,9,11,13	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,7,10,17	2,8,9,11,13,15,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,7,10,16,18	2,8,9,11,13,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,7,10,14	2,8,9,11,13	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,7,10,14,16,17,18	2,8,9,11,13,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,7,10,14,18	2,8,9,11,13,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,7,10,14,16,17	2,8,9,11,13,15,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,7,10,12,18	2,8,9,11,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,7,10,12,16,17	2,8,9,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,7,10,12	2,8,9,11,15	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,7,10,12,16,17,18	2,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,7,10,12,14,17	2,8,9,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,7,10,12,14,16,18	2,8,9,11,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,7,10,12,14,17,18	2,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,7,10,12,14,16	2,8,9,11,15	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,7,10,12	2,8,9,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,7,10,12,16,17,18	2,8,9,11,13,17,18	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,7,10,12,18	2,8,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,7,10,12,16,17	2,8,9,11,13,15,17	2^{-12}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,7,10,12,14,17,18	2,8,9,11,13,17,18	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,7,10,12,14,16	2,8,9,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,7,10,12,14,17	2,8,9,11,13,15,17	2^{-23}
$(1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,7,10,12,14,16,18	2,8,9,11,13,15,18	$2^{-17.5}$

Table 0.1825 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3	2,6	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,16,17,18	2,6,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,18	2,6,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,16,17	2,6,15,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,14,17,18	2,6,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,14,16	2,6	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,14,17	2,6,15,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,14,16,18	2,6,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,18	2,6,13,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,16,17	2,6,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3	2,6,13,15	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,16,17,18	2,6,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,14,17	2,6,13,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,14,16,18	2,6,13,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,14,17,18	2,6,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,14,16	2,6,13,15	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,12,17,18	2,6,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,12,16	2,6	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,12,17	2,6,15,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,12,16,18	2,6,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,12,14	2,6	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,12,14,16,17,18	2,6,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,12,14,18	2,6,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,12,14,16,17	2,6,15,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,12,17	2,6,13,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,12,16,18	2,6,13,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,12,17,18	2,6,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,12,16	2,6,13,15	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,12,14,18	2,6,13,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,12,14,16,17	2,6,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,12,14	2,6,13,15	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,12,14,16,17,18	2,6,13,15,17,18	$2^{-17.5}$

Table 0.1826 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,18	2,6,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,16,17	2,6,11,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3	2,6,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,16,17,18	2,6,11,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,14,17	2,6,11,17	2^{-1}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,14,16,18	2,6,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,14,17,18	2,6,11,15,17,18	2^{-1}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,14,16	2,6,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3	2,6,11,13	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,16,17,18	2,6,11,13,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,18	2,6,11,13,15,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,16,17	2,6,11,13,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,14,17,18	2,6,11,13,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,14,16	2,6,11,13	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,14,17	2,6,11,13,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,14,16,18	2,6,11,13,15,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,12,17	2,6,11,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,12,16,18	2,6,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,12,17,18	2,6,11,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,12,16	2,6,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,12,14,18	2,6,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,12,14,16,17	2,6,11,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,12,14	2,6,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,12,14,16,17,18	2,6,11,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,12,17,18	2,6,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,12,16	2,6,11,13	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,12,17	2,6,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,12,16,18	2,6,11,13,15,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,12,14	2,6,11,13	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,12,14,16,17,18	2,6,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,12,14,18	2,6,11,13,15,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,12,14,16,17	2,6,11,13,15,17	$2^{-17.5}$

Table 0.1827 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,10,17,18	2,6,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,10,16	2,6	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,10,17	2,6,15,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,10,16,18	2,6,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,10,14	2,6	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,10,14,16,17,18	2,6,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,10,14,18	2,6,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,10,14,16,17	2,6,15,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,10,17	2,6,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,10,16,18	2,6,13,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,10,17,18	2,6,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,10,16	2,6,13,15	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,10,14,18	2,6,13,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,10,14,16,17	2,6,13,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,10,14	2,6,13,15	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,10,14,16,17,18	2,6,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,10,12	2,6	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,10,12,16,17,18	2,6,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,10,12,18	2,6,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,10,12,16,17	2,6,15,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,10,12,14,17,18	2,6,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,10,12,14,16	2,6	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,10,12,14,17	2,6,15,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,10,12,14,16,18	2,6,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,10,12,18	2,6,13,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,10,12,16,17	2,6,13,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,10,12	2,6,13,15	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,10,12,16,17,18	2,6,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,10,12,14,17	2,6,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,10,12,14,16,18	2,6,13,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,10,12,14,17,18	2,6,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,10,12,14,16	2,6,13,15	2^{-23}

Table 0.1828 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,10,17	2,6,11,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,10,16,18	2,6,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,10,17,18	2,6,11,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,10,16	2,6,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,10,14,18	2,6,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,10,14,16,17	2,6,11,17	2^{-34}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,10,14	2,6,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,10,14,16,17,18	2,6,11,15,17,18	2^{-34}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,10,17,18	2,6,11,13,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,10,16	2,6,11,13	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,10,17	2,6,11,13,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,10,16,18	2,6,11,13,15,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,10,14	2,6,11,13	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,10,14,16,17,18	2,6,11,13,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,10,14,18	2,6,11,13,15,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,10,14,16,17	2,6,11,13,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,10,12,18	2,6,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,10,12,16,17	2,6,11,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,10,12	2,6,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,10,12,16,17,18	2,6,11,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,10,12,14,17	2,6,11,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,10,12,14,16,18	2,6,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,10,12,14,17,18	2,6,11,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,10,12,14,16	2,6,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,10,12	2,6,11,13	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,10,12,16,17,18	2,6,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,10,12,18	2,6,11,13,15,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,10,12,16,17	2,6,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,10,12,14,17,18	2,6,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,10,12,14,16	2,6,11,13	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,10,12,14,17	2,6,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,10,12,14,16,18	2,6,11,13,15,18	2^{-23}

Table 0.1829 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,18	2,6,9,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,16,17	2,6,9,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3	2,6,9,15	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,16,17,18	2,6,9,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,14,17	2,6,9,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,14,16,18	2,6,9,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,14,17,18	2,6,9,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,14,16	2,6,9,15	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3	2,6,9,13	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,16,17,18	2,6,9,13,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,18	2,6,9,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,16,17	2,6,9,13,15,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,14,17,18	2,6,9,13,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,14,16	2,6,9,13	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,14,17	2,6,9,13,15,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,14,16,18	2,6,9,13,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,12,17	2,6,9,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,12,16,18	2,6,9,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,12,17,18	2,6,9,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,12,16	2,6,9,15	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,12,14,18	2,6,9,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,12,14,16,17	2,6,9,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,12,14	2,6,9,15	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,12,14,16,17,18	2,6,9,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,12,17,18	2,6,9,13,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,12,16	2,6,9,13	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,12,17	2,6,9,13,15,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,12,16,18	2,6,9,13,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,12,14	2,6,9,13	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,12,14,16,17,18	2,6,9,13,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,12,14,18	2,6,9,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,12,14,16,17	2,6,9,13,15,17	2^{-23}

Table 0.1830 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3	2,6,9,11	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,16,17,18	2,6,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,18	2,6,9,11,15,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,16,17	2,6,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,14,17,18	2,6,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,14,16	2,6,9,11	2^{-34}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,14,17	2,6,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,14,16,18	2,6,9,11,15,18	2^{-34}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,18	2,6,9,11,13,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,16,17	2,6,9,11,13,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3	2,6,9,11,13,15	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,16,17,18	2,6,9,11,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,14,17	2,6,9,11,13,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,14,16,18	2,6,9,11,13,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,14,17,18	2,6,9,11,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,14,16	2,6,9,11,13,15	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,12,17,18	2,6,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,12,16	2,6,9,11	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,12,17	2,6,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,12,16,18	2,6,9,11,15,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,12,14	2,6,9,11	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,12,14,16,17,18	2,6,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,12,14,18	2,6,9,11,15,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,12,14,16,17	2,6,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,12,17	2,6,9,11,13,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,12,16,18	2,6,9,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,12,17,18	2,6,9,11,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,12,16	2,6,9,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,12,14,18	2,6,9,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,12,14,16,17	2,6,9,11,13,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,12,14	2,6,9,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,12,14,16,17,18	2,6,9,11,13,15,17,18	2^{-23}

Table 0.1831 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,10,17	2,6,9,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,10,16,18	2,6,9,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,10,17,18	2,6,9,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,10,16	2,6,9,15	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,10,14,18	2,6,9,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,10,14,16,17	2,6,9,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,10,14	2,6,9,15	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,10,14,16,17,18	2,6,9,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,10,17,18	2,6,9,13,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,10,16	2,6,9,13	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,10,17	2,6,9,13,15,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,10,16,18	2,6,9,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,10,14	2,6,9,13	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,10,14,16,17,18	2,6,9,13,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,10,14,18	2,6,9,13,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,10,14,16,17	2,6,9,13,15,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,10,12,18	2,6,9,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,10,12,16,17	2,6,9,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,10,12	2,6,9,15	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,10,12,16,17,18	2,6,9,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,10,12,14,17	2,6,9,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,10,12,14,16,18	2,6,9,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,10,12,14,17,18	2,6,9,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,10,12,14,16	2,6,9,15	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,10,12	2,6,9,13	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,10,12,16,17,18	2,6,9,13,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,10,12,18	2,6,9,13,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,10,12,16,17	2,6,9,13,15,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,10,12,14,17,18	2,6,9,13,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,10,12,14,16	2,6,9,13	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,10,12,14,17	2,6,9,13,15,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,10,12,14,16,18	2,6,9,13,15,18	$2^{-17.5}$

Table 0.1832 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,10,17,18	2,6,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,10,16	2,6,9,11	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,10,17	2,6,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,10,16,18	2,6,9,11,15,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,10,14	2,6,9,11	2^{-1}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,10,14,16,17,18	2,6,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,10,14,18	2,6,9,11,15,18	2^{-1}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,10,14,16,17	2,6,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,10,17	2,6,9,11,13,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,10,16,18	2,6,9,11,13,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,10,17,18	2,6,9,11,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,10,16	2,6,9,11,13,15	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,10,14,18	2,6,9,11,13,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,10,14,16,17	2,6,9,11,13,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,10,14	2,6,9,11,13,15	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,10,14,16,17,18	2,6,9,11,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,10,12	2,6,9,11	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,10,12,16,17,18	2,6,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,10,12,18	2,6,9,11,15,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,10,12,16,17	2,6,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,10,12,14,17,18	2,6,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,10,12,14,16	2,6,9,11	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,10,12,14,17	2,6,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,10,12,14,16,18	2,6,9,11,15,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,10,12,18	2,6,9,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,10,12,16,17	2,6,9,11,13,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,10,12	2,6,9,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,10,12,16,17,18	2,6,9,11,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,10,12,14,17	2,6,9,11,13,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,10,12,14,16,18	2,6,9,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,10,12,14,17,18	2,6,9,11,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,10,12,14,16	2,6,9,11,13,15	$2^{-17.5}$

Table 0.1833 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,17,18	2,6,8,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,16	2,6,8	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,17	2,6,8,15,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,16,18	2,6,8,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,14	2,6,8	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,14,16,17,18	2,6,8,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,14,18	2,6,8,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,14,16,17	2,6,8,15,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,17	2,6,8,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,16,18	2,6,8,13,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,17,18	2,6,8,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,16	2,6,8,13,15	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,14,18	2,6,8,13,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,14,16,17	2,6,8,13,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,14	2,6,8,13,15	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,14,16,17,18	2,6,8,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,12	2,6,8	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,12,16,17,18	2,6,8,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,12,18	2,6,8,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,12,16,17	2,6,8,15,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,12,14,17,18	2,6,8,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,12,14,16	2,6,8	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,12,14,17	2,6,8,15,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,12,14,16,18	2,6,8,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,12,18	2,6,8,13,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,12,16,17	2,6,8,13,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,12	2,6,8,13,15	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,12,16,17,18	2,6,8,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,12,14,17	2,6,8,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,12,14,16,18	2,6,8,13,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,12,14,17,18	2,6,8,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,12,14,16	2,6,8,13,15	2^{-12}

Table 0.1834 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,17	2,6,8,11,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,16,18	2,6,8,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,17,18	2,6,8,11,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,16	2,6,8,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,14,18	2,6,8,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,14,16,17	2,6,8,11,17	2^{-1}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,14	2,6,8,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,14,16,17,18	2,6,8,11,15,17,18	2^{-1}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,17,18	2,6,8,11,13,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,16	2,6,8,11,13	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,17	2,6,8,11,13,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,16,18	2,6,8,11,13,15,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,14	2,6,8,11,13	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,14,16,17,18	2,6,8,11,13,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,14,18	2,6,8,11,13,15,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,14,16,17	2,6,8,11,13,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,12,18	2,6,8,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,12,16,17	2,6,8,11,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,12	2,6,8,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,12,16,17,18	2,6,8,11,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,12,14,17	2,6,8,11,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,12,14,16,18	2,6,8,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,12,14,17,18	2,6,8,11,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,12,14,16	2,6,8,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,12	2,6,8,11,13	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,12,16,17,18	2,6,8,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,12,18	2,6,8,11,13,15,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,12,16,17	2,6,8,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,12,14,17,18	2,6,8,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,12,14,16	2,6,8,11,13	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,12,14,17	2,6,8,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,12,14,16,18	2,6,8,11,13,15,18	2^{-12}

Table 0.1835 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,10	2,6,8	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,10,16,17,18	2,6,8,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,10,18	2,6,8,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,10,16,17	2,6,8,15,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,10,14,17,18	2,6,8,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,10,14,16	2,6,8	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,10,14,17	2,6,8,15,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,10,14,16,18	2,6,8,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,10,18	2,6,8,13,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,10,16,17	2,6,8,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,10	2,6,8,13,15	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,10,16,17,18	2,6,8,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,10,14,17	2,6,8,13,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,10,14,16,18	2,6,8,13,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,10,14,17,18	2,6,8,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,10,14,16	2,6,8,13,15	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,10,12,17,18	2,6,8,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,10,12,16	2,6,8	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,10,12,17	2,6,8,15,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,10,12,16,18	2,6,8,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,10,12,14	2,6,8	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,10,12,14,16,17,18	2,6,8,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,10,12,14,18	2,6,8,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,10,12,14,16,17	2,6,8,15,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,10,12,17	2,6,8,13,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,10,12,16,18	2,6,8,13,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,10,12,17,18	2,6,8,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,10,12,16	2,6,8,13,15	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,10,12,14,18	2,6,8,13,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,10,12,14,16,17	2,6,8,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,10,12,14	2,6,8,13,15	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,10,12,14,16,17,18	2,6,8,13,15,17,18	$2^{-17.5}$

Table 0.1836 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,10,18	2,6,8,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,10,16,17	2,6,8,11,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,10	2,6,8,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,10,16,17,18	2,6,8,11,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,10,14,17	2,6,8,11,17	2^{-34}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,10,14,16,18	2,6,8,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,10,14,17,18	2,6,8,11,15,17,18	2^{-34}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,10,14,16	2,6,8,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,10	2,6,8,11,13	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,10,16,17,18	2,6,8,11,13,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,10,18	2,6,8,11,13,15,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,10,16,17	2,6,8,11,13,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,10,14,17,18	2,6,8,11,13,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,10,14,16	2,6,8,11,13	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,10,14,17	2,6,8,11,13,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,10,14,16,18	2,6,8,11,13,15,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,10,12,17	2,6,8,11,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,10,12,16,18	2,6,8,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,10,12,17,18	2,6,8,11,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,10,12,16	2,6,8,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,10,12,14,18	2,6,8,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,10,12,14,16,17	2,6,8,11,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,10,12,14	2,6,8,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,10,12,14,16,17,18	2,6,8,11,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,10,12,17,18	2,6,8,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,10,12,16	2,6,8,11,13	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,10,12,17	2,6,8,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,10,12,16,18	2,6,8,11,13,15,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,10,12,14	2,6,8,11,13	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,10,12,14,16,17,18	2,6,8,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,10,12,14,18	2,6,8,11,13,15,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,10,12,14,16,17	2,6,8,11,13,15,17	$2^{-17.5}$

Table 0.1837 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,17	2,6,8,9,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,16,18	2,6,8,9,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,17,18	2,6,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,16	2,6,8,9,15	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,14,18	2,6,8,9,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,14,16,17	2,6,8,9,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,14	2,6,8,9,15	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,14,16,17,18	2,6,8,9,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,17,18	2,6,8,9,13,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,16	2,6,8,9,13	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,17	2,6,8,9,13,15,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,16,18	2,6,8,9,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,14	2,6,8,9,13	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,14,16,17,18	2,6,8,9,13,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,14,18	2,6,8,9,13,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,14,16,17	2,6,8,9,13,15,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,12,18	2,6,8,9,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,12,16,17	2,6,8,9,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0)$	1,3,12	2,6,8,9,15	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,12,16,17,18	2,6,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,12,14,17	2,6,8,9,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,12,14,16,18	2,6,8,9,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,12,14,17,18	2,6,8,9,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,12,14,16	2,6,8,9,15	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,12	2,6,8,9,13	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,12,16,17,18	2,6,8,9,13,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,12,18	2,6,8,9,13,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,12,16,17	2,6,8,9,13,15,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,12,14,17,18	2,6,8,9,13,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,12,14,16	2,6,8,9,13	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,12,14,17	2,6,8,9,13,15,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,12,14,16,18	2,6,8,9,13,15,18	$2^{-17.5}$

Table 0.1838 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,17,18	2,6,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,16	2,6,8,9,11	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,17	2,6,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,16,18	2,6,8,9,11,15,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,14	2,6,8,9,11	2^{-34}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,14,16,17,18	2,6,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,14,18	2,6,8,9,11,15,18	2^{-34}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,14,16,17	2,6,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,17	2,6,8,9,11,13,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,16,18	2,6,8,9,11,13,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,17,18	2,6,8,9,11,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,16	2,6,8,9,11,13,15	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,14,18	2,6,8,9,11,13,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,14,16,17	2,6,8,9,11,13,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,14	2,6,8,9,11,13,15	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,14,16,17,18	2,6,8,9,11,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,12	2,6,8,9,11	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,12,16,17,18	2,6,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,12,18	2,6,8,9,11,15,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,12,16,17	2,6,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,12,14,17,18	2,6,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,12,14,16	2,6,8,9,11	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,12,14,17	2,6,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,12,14,16,18	2,6,8,9,11,15,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,12,18	2,6,8,9,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,12,16,17	2,6,8,9,11,13,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,12	2,6,8,9,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,12,16,17,18	2,6,8,9,11,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,12,14,17	2,6,8,9,11,13,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,12,14,16,18	2,6,8,9,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,12,14,17,18	2,6,8,9,11,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,12,14,16	2,6,8,9,11,13,15	$2^{-17.5}$

Table 0.1839 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,10,18	2,6,8,9,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,10,16,17	2,6,8,9,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,10	2,6,8,9,15	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,10,16,17,18	2,6,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,10,14,17	2,6,8,9,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,10,14,16,18	2,6,8,9,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,10,14,17,18	2,6,8,9,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,10,14,16	2,6,8,9,15	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,10	2,6,8,9,13	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,10,16,17,18	2,6,8,9,13,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,10,18	2,6,8,9,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,10,16,17	2,6,8,9,13,15,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,10,14,17,18	2,6,8,9,13,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,10,14,16	2,6,8,9,13	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,10,14,17	2,6,8,9,13,15,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,10,14,16,18	2,6,8,9,13,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,10,12,17	2,6,8,9,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,10,12,16,18	2,6,8,9,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,10,12,17,18	2,6,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,10,12,16	2,6,8,9,15	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,10,12,14,18	2,6,8,9,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,10,12,14,16,17	2,6,8,9,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,10,12,14	2,6,8,9,15	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,10,12,14,16,17,18	2,6,8,9,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,10,12,17,18	2,6,8,9,13,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,10,12,16	2,6,8,9,13	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,10,12,17	2,6,8,9,13,15,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,10,12,16,18	2,6,8,9,13,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,10,12,14	2,6,8,9,13	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,10,12,14,16,17,18	2,6,8,9,13,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,10,12,14,18	2,6,8,9,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,10,12,14,16,17	2,6,8,9,13,15,17	2^{-12}

Table 0.1840 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,10	2,6,8,9,11	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,10,16,17,18	2,6,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,10,18	2,6,8,9,11,15,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,10,16,17	2,6,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,10,14,17,18	2,6,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,10,14,16	2,6,8,9,11	2^{-1}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,10,14,17	2,6,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,10,14,16,18	2,6,8,9,11,15,18	2^{-1}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,10,18	2,6,8,9,11,13,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,10,16,17	2,6,8,9,11,13,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,10	2,6,8,9,11,13,15	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,10,16,17,18	2,6,8,9,11,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,10,14,17	2,6,8,9,11,13,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,10,14,16,18	2,6,8,9,11,13,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,10,14,17,18	2,6,8,9,11,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,10,14,16	2,6,8,9,11,13,15	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,10,12,17,18	2,6,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,10,12,16	2,6,8,9,11	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,10,12,17	2,6,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,10,12,16,18	2,6,8,9,11,15,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,10,12,14	2,6,8,9,11	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,10,12,14,16,17,18	2,6,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,10,12,14,18	2,6,8,9,11,15,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,10,12,14,16,17	2,6,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,10,12,17	2,6,8,9,11,13,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,10,12,16,18	2,6,8,9,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,10,12,17,18	2,6,8,9,11,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,10,12,16	2,6,8,9,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,10,12,14,18	2,6,8,9,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,10,12,14,16,17	2,6,8,9,11,13,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,10,12,14	2,6,8,9,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,10,12,14,16,17,18	2,6,8,9,11,13,15,17,18	2^{-12}

Table 0.1841 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,7,18	2,6,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,7,16,17	2,6,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,7	2,6,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0)$	1,3,7,16,17,18	2,6,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)$	1,3,7,14,17	2,6,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,7,14,16,18	2,6,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,7,14,17,18	2,6,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,7,14,16	2,6,15	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,7	2,6,13	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,7,16,17,18	2,6,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,7,18	2,6,13,15,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,7,16,17	2,6,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1)$	1,3,7,14,17,18	2,6,13,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,7,14,16	2,6,13	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,7,14,17	2,6,13,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,7,14,16,18	2,6,13,15,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,7,12,17	2,6,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,7,12,16,18	2,6,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,7,12,17,18	2,6,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,7,12,16	2,6,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,7,12,14,18	2,6,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,7,12,14,16,17	2,6,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0)$	1,3,7,12,14	2,6,15	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0)$	1,3,7,12,14,16,17,18	2,6,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,7,12,17,18	2,6,13,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,7,12,16	2,6,13	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,7,12,17	2,6,13,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,7,12,16,18	2,6,13,15,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,7,12,14	2,6,13	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,7,12,14,16,17,18	2,6,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,7,12,14,18	2,6,13,15,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0)$	1,3,7,12,14,16,17	2,6,13,15,17	$2^{-17.5}$

Table 0.1842 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,7	2,6,11	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,7,16,17,18	2,6,11,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,7,18	2,6,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,7,16,17	2,6,11,15,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,7,14,17,18	2,6,11,17,18	2^{-1}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,7,14,16	2,6,11	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,7,14,17	2,6,11,15,17	2^{-1}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,7,14,16,18	2,6,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,7,18	2,6,11,13,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,7,16,17	2,6,11,13,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,7	2,6,11,13,15	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,7,16,17,18	2,6,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,7,14,17	2,6,11,13,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,7,14,16,18	2,6,11,13,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,7,14,17,18	2,6,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,7,14,16	2,6,11,13,15	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,7,12,17,18	2,6,11,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,7,12,16	2,6,11	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,7,12,17	2,6,11,15,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,7,12,16,18	2,6,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,7,12,14	2,6,11	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,7,12,14,16,17,18	2,6,11,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,7,12,14,18	2,6,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,7,12,14,16,17	2,6,11,15,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,7,12,17	2,6,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,7,12,16,18	2,6,11,13,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,7,12,17,18	2,6,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,7,12,16	2,6,11,13,15	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,7,12,14,18	2,6,11,13,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,7,12,14,16,17	2,6,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,7,12,14	2,6,11,13,15	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,7,12,14,16,17,18	2,6,11,13,15,17,18	$2^{-17.5}$

Table 0.1843 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,7,10,17	2,6,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,7,10,16,18	2,6,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,7,10,17,18	2,6,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,7,10,16	2,6,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,7,10,14,18	2,6,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,7,10,14,16,17	2,6,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,7,10,14	2,6,15	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,7,10,14,16,17,18	2,6,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,7,10,17,18	2,6,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,7,10,16	2,6,13	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,7,10,17	2,6,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,7,10,16,18	2,6,13,15,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,7,10,14	2,6,13	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,7,10,14,16,17,18	2,6,13,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,7,10,14,18	2,6,13,15,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,7,10,14,16,17	2,6,13,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,7,10,12,18	2,6,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,7,10,12,16,17	2,6,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,7,10,12	2,6,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,7,10,12,16,17,18	2,6,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,7,10,12,14,17	2,6,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,7,10,12,14,16,18	2,6,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,7,10,12,14,17,18	2,6,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,7,10,12,14,16	2,6,15	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,7,10,12	2,6,13	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,7,10,12,16,17,18	2,6,13,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,7,10,12,18	2,6,13,15,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,7,10,12,16,17	2,6,13,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,7,10,12,14,17,18	2,6,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,7,10,12,14,16	2,6,13	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,7,10,12,14,17	2,6,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,7,10,12,14,16,18	2,6,13,15,18	2^{-23}

Table 0.1844 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,7,10,17,18	2,6,11,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,7,10,16	2,6,11	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,7,10,17	2,6,11,15,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,7,10,16,18	2,6,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,7,10,14	2,6,11	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,7,10,14,16,17,18	2,6,11,17,18	2^{-34}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,7,10,14,18	2,6,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,7,10,14,16,17	2,6,11,15,17	2^{-34}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,7,10,17	2,6,11,13,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,7,10,16,18	2,6,11,13,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,7,10,17,18	2,6,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,7,10,16	2,6,11,13,15	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,7,10,14,18	2,6,11,13,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,7,10,14,16,17	2,6,11,13,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,7,10,14	2,6,11,13,15	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,7,10,14,16,17,18	2,6,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,7,10,12	2,6,11	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,7,10,12,16,17,18	2,6,11,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,7,10,12,18	2,6,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,7,10,12,16,17	2,6,11,15,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,7,10,12,14,17,18	2,6,11,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,7,10,12,14,16	2,6,11	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,7,10,12,14,17	2,6,11,15,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,7,10,12,14,16,18	2,6,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,7,10,12,18	2,6,11,13,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,7,10,12,16,17	2,6,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,7,10,12	2,6,11,13,15	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,7,10,12,16,17,18	2,6,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,10,12,14,17	2,6,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,7,10,12,14,16,18	2,6,11,13,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,10,12,14,17,18	2,6,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,7,10,12,14,16	2,6,11,13,15	2^{-23}

Table 0.1845 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,7	2,6,9	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,7,16,17,18	2,6,9,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,7,18	2,6,9,15,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,7,16,17	2,6,9,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,7,14,17,18	2,6,9,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,7,14,16	2,6,9	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,7,14,17	2,6,9,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,7,14,16,18	2,6,9,15,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,7,18	2,6,9,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,7,16,17	2,6,9,13,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,7	2,6,9,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,7,16,17,18	2,6,9,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,7,14,17	2,6,9,13,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,7,14,16,18	2,6,9,13,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,7,14,17,18	2,6,9,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,7,14,16	2,6,9,13,15	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,7,12,17,18	2,6,9,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,7,12,16	2,6,9	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,7,12,17	2,6,9,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,7,12,16,18	2,6,9,15,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,7,12,14	2,6,9	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,7,12,14,16,17,18	2,6,9,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,7,12,14,18	2,6,9,15,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,7,12,14,16,17	2,6,9,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,7,12,17	2,6,9,13,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,7,12,16,18	2,6,9,13,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,7,12,17,18	2,6,9,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,7,12,16	2,6,9,13,15	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,7,12,14,18	2,6,9,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,7,12,14,16,17	2,6,9,13,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,7,12,14	2,6,9,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,7,12,14,16,17,18	2,6,9,13,15,17,18	2^{-23}

Table 0.1846 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,7,18	2,6,9,11,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,7,16,17	2,6,9,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,7	2,6,9,11,15	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,7,16,17,18	2,6,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,7,14,17	2,6,9,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,7,14,16,18	2,6,9,11,18	2^{-34}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,7,14,17,18	2,6,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,7,14,16	2,6,9,11,15	2^{-34}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,7	2,6,9,11,13	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,7,16,17,18	2,6,9,11,13,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,7,18	2,6,9,11,13,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,7,16,17	2,6,9,11,13,15,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,7,14,17,18	2,6,9,11,13,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,7,14,16	2,6,9,11,13	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,7,14,17	2,6,9,11,13,15,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,7,14,16,18	2,6,9,11,13,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,7,12,17	2,6,9,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,7,12,16,18	2,6,9,11,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,7,12,17,18	2,6,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,7,12,16	2,6,9,11,15	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,7,12,14,18	2,6,9,11,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,7,12,14,16,17	2,6,9,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,7,12,14	2,6,9,11,15	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,7,12,14,16,17,18	2,6,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,7,12,17,18	2,6,9,11,13,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,7,12,16	2,6,9,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,7,12,17	2,6,9,11,13,15,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,7,12,16,18	2,6,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,7,12,14	2,6,9,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,7,12,14,16,17,18	2,6,9,11,13,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0)$	1,3,7,12,14,18	2,6,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,7,12,14,16,17	2,6,9,11,13,15,17	2^{-23}

Table 0.1847 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,7,10,17,18	2,6,9,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,7,10,16	2,6,9	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,7,10,17	2,6,9,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,7,10,16,18	2,6,9,15,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,7,10,14	2,6,9	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,7,10,14,16,17,18	2,6,9,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,7,10,14,18	2,6,9,15,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,7,10,14,16,17	2,6,9,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,7,10,17	2,6,9,13,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,7,10,16,18	2,6,9,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,7,10,17,18	2,6,9,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,7,10,16	2,6,9,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,7,10,14,18	2,6,9,13,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,7,10,14,16,17	2,6,9,13,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,7,10,14	2,6,9,13,15	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,7,10,14,16,17,18	2,6,9,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,7,10,12	2,6,9	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,7,10,12,16,17,18	2,6,9,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,7,10,12,18	2,6,9,15,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,7,10,12,16,17	2,6,9,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,7,10,12,14,17,18	2,6,9,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,7,10,12,14,16	2,6,9	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,7,10,12,14,17	2,6,9,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,7,10,12,14,16,18	2,6,9,15,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,7,10,12,18	2,6,9,13,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,7,10,12,16,17	2,6,9,13,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,7,10,12	2,6,9,13,15	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,7,10,12,16,17,18	2,6,9,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,10,12,14,17	2,6,9,13,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,7,10,12,14,16,18	2,6,9,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,10,12,14,17,18	2,6,9,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,7,10,12,14,16	2,6,9,13,15	$2^{-17.5}$

Table 0.1848 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,7,10,17	2,6,9,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,7,10,16,18	2,6,9,11,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,7,10,17,18	2,6,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,7,10,16	2,6,9,11,15	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,7,10,14,18	2,6,9,11,18	2^{-1}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,7,10,14,16,17	2,6,9,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,7,10,14	2,6,9,11,15	2^{-1}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,7,10,14,16,17,18	2,6,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,7,10,17,18	2,6,9,11,13,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,7,10,16	2,6,9,11,13	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,7,10,17	2,6,9,11,13,15,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,7,10,16,18	2,6,9,11,13,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,7,10,14	2,6,9,11,13	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,7,10,14,16,17,18	2,6,9,11,13,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,7,10,14,18	2,6,9,11,13,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,7,10,14,16,17	2,6,9,11,13,15,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,7,10,12,18	2,6,9,11,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,7,10,12,16,17	2,6,9,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,7,10,12	2,6,9,11,15	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,7,10,12,16,17,18	2,6,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,7,10,12,14,17	2,6,9,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,7,10,12,14,16,18	2,6,9,11,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,7,10,12,14,17,18	2,6,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,7,10,12,14,16	2,6,9,11,15	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,7,10,12	2,6,9,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,7,10,12,16,17,18	2,6,9,11,13,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,7,10,12,18	2,6,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,7,10,12,16,17	2,6,9,11,13,15,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,7,10,12,14,17,18	2,6,9,11,13,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,7,10,12,14,16	2,6,9,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,7,10,12,14,17	2,6,9,11,13,15,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,7,10,12,14,16,18	2,6,9,11,13,15,18	$2^{-17.5}$

Table 0.1849 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,7,17	2,6,8,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,7,16,18	2,6,8,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,7,17,18	2,6,8,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,7,16	2,6,8,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,7,14,18	2,6,8,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,7,14,16,17	2,6,8,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,7,14	2,6,8,15	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,7,14,16,17,18	2,6,8,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,7,17,18	2,6,8,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,7,16	2,6,8,13	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,7,17	2,6,8,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,7,16,18	2,6,8,13,15,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,7,14	2,6,8,13	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,7,14,16,17,18	2,6,8,13,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,7,14,18	2,6,8,13,15,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,7,14,16,17	2,6,8,13,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,7,12,18	2,6,8,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,7,12,16,17	2,6,8,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,7,12	2,6,8,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,7,12,16,17,18	2,6,8,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,7,12,14,17	2,6,8,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,7,12,14,16,18	2,6,8,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,7,12,14,17,18	2,6,8,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,7,12,14,16	2,6,8,15	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,7,12	2,6,8,13	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,7,12,16,17,18	2,6,8,13,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,7,12,18	2,6,8,13,15,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,7,12,16,17	2,6,8,13,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,7,12,14,17,18	2,6,8,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,12,14,16	2,6,8,13	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,7,12,14,17	2,6,8,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,12,14,16,18	2,6,8,13,15,18	2^{-12}

Table 0.1850 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,7,17,18	2,6,8,11,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,7,16	2,6,8,11	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,7,17	2,6,8,11,15,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,7,16,18	2,6,8,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,7,14	2,6,8,11	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,7,14,16,17,18	2,6,8,11,17,18	2^{-1}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,7,14,18	2,6,8,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,7,14,16,17	2,6,8,11,15,17	2^{-1}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,7,17	2,6,8,11,13,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,7,16,18	2,6,8,11,13,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,7,17,18	2,6,8,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,7,16	2,6,8,11,13,15	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,7,14,18	2,6,8,11,13,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,7,14,16,17	2,6,8,11,13,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,7,14	2,6,8,11,13,15	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,7,14,16,17,18	2,6,8,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,7,12	2,6,8,11	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,7,12,16,17,18	2,6,8,11,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,7,12,18	2,6,8,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,7,12,16,17	2,6,8,11,15,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,7,12,14,17,18	2,6,8,11,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,7,12,14,16	2,6,8,11	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,7,12,14,17	2,6,8,11,15,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,7,12,14,16,18	2,6,8,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,7,12,18	2,6,8,11,13,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,7,12,16,17	2,6,8,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,7,12	2,6,8,11,13,15	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,7,12,16,17,18	2,6,8,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,7,12,14,17	2,6,8,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,7,12,14,16,18	2,6,8,11,13,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,7,12,14,17,18	2,6,8,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,7,12,14,16	2,6,8,11,13,15	2^{-12}

Table 0.1851 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,7,10,18	2,6,8,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,7,10,16,17	2,6,8,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,7,10	2,6,8,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,7,10,16,17,18	2,6,8,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,7,10,14,17	2,6,8,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,7,10,14,16,18	2,6,8,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,7,10,14,17,18	2,6,8,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,7,10,14,16	2,6,8,15	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,7,10	2,6,8,13	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,7,10,16,17,18	2,6,8,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,7,10,18	2,6,8,13,15,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,7,10,16,17	2,6,8,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,7,10,14,17,18	2,6,8,13,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,7,10,14,16	2,6,8,13	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,7,10,14,17	2,6,8,13,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,7,10,14,16,18	2,6,8,13,15,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,7,10,12,17	2,6,8,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,7,10,12,16,18	2,6,8,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1)$	1,3,7,10,12,17,18	2,6,8,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,7,10,12,16	2,6,8,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,7,10,12,14,18	2,6,8,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,7,10,12,14,16,17	2,6,8,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,7,10,12,14	2,6,8,15	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,7,10,12,14,16,17,18	2,6,8,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,7,10,12,17,18	2,6,8,13,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,7,10,12,16	2,6,8,13	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,7,10,12,17	2,6,8,13,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,7,10,12,16,18	2,6,8,13,15,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,7,10,12,14	2,6,8,13	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,7,10,12,14,16,17,18	2,6,8,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,7,10,12,14,18	2,6,8,13,15,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,7,10,12,14,16,17	2,6,8,13,15,17	$2^{-17.5}$

Table 0.1852 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,7,10	2,6,8,11	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,7,10,16,17,18	2,6,8,11,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,7,10,18	2,6,8,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,7,10,16,17	2,6,8,11,15,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,7,10,14,17,18	2,6,8,11,17,18	2^{-34}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,7,10,14,16	2,6,8,11	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,7,10,14,17	2,6,8,11,15,17	2^{-34}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,7,10,14,16,18	2,6,8,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,7,10,18	2,6,8,11,13,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,7,10,16,17	2,6,8,11,13,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,7,10	2,6,8,11,13,15	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,7,10,16,17,18	2,6,8,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,7,10,14,17	2,6,8,11,13,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,7,10,14,16,18	2,6,8,11,13,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,7,10,14,17,18	2,6,8,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,7,10,14,16	2,6,8,11,13,15	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,7,10,12,17,18	2,6,8,11,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,7,10,12,16	2,6,8,11	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,7,10,12,17	2,6,8,11,15,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,7,10,12,16,18	2,6,8,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,7,10,12,14	2,6,8,11	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,7,10,12,14,16,17,18	2,6,8,11,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,7,10,12,14,18	2,6,8,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,7,10,12,14,16,17	2,6,8,11,15,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,7,10,12,17	2,6,8,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,7,10,12,16,18	2,6,8,11,13,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,7,10,12,17,18	2,6,8,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,7,10,12,16	2,6,8,11,13,15	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,7,10,12,14,18	2,6,8,11,13,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,7,10,12,14,16,17	2,6,8,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,7,10,12,14	2,6,8,11,13,15	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,7,10,12,14,16,17,18	2,6,8,11,13,15,17,18	$2^{-17.5}$

Table 0.1853 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,7,17,18	2,6,8,9,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,7,16	2,6,8,9	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,7,17	2,6,8,9,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,7,16,18	2,6,8,9,15,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,7,14	2,6,8,9	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,7,14,16,17,18	2,6,8,9,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,7,14,18	2,6,8,9,15,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,7,14,16,17	2,6,8,9,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,7,17	2,6,8,9,13,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,7,16,18	2,6,8,9,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,7,17,18	2,6,8,9,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,7,16	2,6,8,9,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,7,14,18	2,6,8,9,13,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,7,14,16,17	2,6,8,9,13,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,7,14	2,6,8,9,13,15	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,7,14,16,17,18	2,6,8,9,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,7,12	2,6,8,9	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,7,12,16,17,18	2,6,8,9,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,7,12,18	2,6,8,9,15,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,7,12,16,17	2,6,8,9,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,7,12,14,17,18	2,6,8,9,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,7,12,14,16	2,6,8,9	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,7,12,14,17	2,6,8,9,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,7,12,14,16,18	2,6,8,9,15,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,7,12,18	2,6,8,9,13,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,7,12,16,17	2,6,8,9,13,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,7,12	2,6,8,9,13,15	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,7,12,16,17,18	2,6,8,9,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,7,12,14,17	2,6,8,9,13,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,7,12,14,16,18	2,6,8,9,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,7,12,14,17,18	2,6,8,9,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,7,12,14,16	2,6,8,9,13,15	$2^{-17.5}$

Table 0.1854 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,7,17	2,6,8,9,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,7,16,18	2,6,8,9,11,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,7,17,18	2,6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,7,16	2,6,8,9,11,15	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,7,14,18	2,6,8,9,11,18	2^{-34}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,7,14,16,17	2,6,8,9,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,7,14	2,6,8,9,11,15	2^{-34}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,7,14,16,17,18	2,6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,7,17,18	2,6,8,9,11,13,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,7,16	2,6,8,9,11,13	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,7,17	2,6,8,9,11,13,15,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,7,16,18	2,6,8,9,11,13,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,7,14	2,6,8,9,11,13	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,7,14,16,17,18	2,6,8,9,11,13,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,7,14,18	2,6,8,9,11,13,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,7,14,16,17	2,6,8,9,11,13,15,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,7,12,18	2,6,8,9,11,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,7,12,16,17	2,6,8,9,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,7,12	2,6,8,9,11,15	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,7,12,16,17,18	2,6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,7,12,14,17	2,6,8,9,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,7,12,14,16,18	2,6,8,9,11,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,7,12,14,17,18	2,6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,7,12,14,16	2,6,8,9,11,15	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,7,12	2,6,8,9,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,7,12,16,17,18	2,6,8,9,11,13,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,7,12,18	2,6,8,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,7,12,16,17	2,6,8,9,11,13,15,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,7,12,14,17,18	2,6,8,9,11,13,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,7,12,14,16	2,6,8,9,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,7,12,14,17	2,6,8,9,11,13,15,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,7,12,14,16,18	2,6,8,9,11,13,15,18	$2^{-17.5}$

Table 0.1855 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,7,10	2,6,8,9	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,7,10,16,17,18	2,6,8,9,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,7,10,18	2,6,8,9,15,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,7,10,16,17	2,6,8,9,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,7,10,14,17,18	2,6,8,9,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,7,10,14,16	2,6,8,9	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,7,10,14,17	2,6,8,9,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,7,10,14,16,18	2,6,8,9,15,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,7,10,18	2,6,8,9,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0)$	1,3,7,10,16,17	2,6,8,9,13,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,7,10	2,6,8,9,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,7,10,16,17,18	2,6,8,9,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,7,10,14,17	2,6,8,9,13,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,7,10,14,16,18	2,6,8,9,13,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,7,10,14,17,18	2,6,8,9,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,7,10,14,16	2,6,8,9,13,15	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,7,10,12,17,18	2,6,8,9,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,7,10,12,16	2,6,8,9	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,7,10,12,17	2,6,8,9,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,7,10,12,16,18	2,6,8,9,15,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,7,10,12,14	2,6,8,9	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,7,10,12,14,16,17,18	2,6,8,9,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,7,10,12,14,18	2,6,8,9,15,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,7,10,12,14,16,17	2,6,8,9,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,7,10,12,17	2,6,8,9,13,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,7,10,12,16,18	2,6,8,9,13,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,7,10,12,17,18	2,6,8,9,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,7,10,12,16	2,6,8,9,13,15	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,7,10,12,14,18	2,6,8,9,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,7,10,12,14,16,17	2,6,8,9,13,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,7,10,12,14	2,6,8,9,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,7,10,12,14,16,17,18	2,6,8,9,13,15,17,18	2^{-12}

Table 0.1856 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,7,10,18	2,6,8,9,11,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,7,10,16,17	2,6,8,9,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,7,10	2,6,8,9,11,15	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,7,10,16,17,18	2,6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,7,10,14,17	2,6,8,9,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,7,10,14,16,18	2,6,8,9,11,18	2^{-1}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,7,10,14,17,18	2,6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,7,10,14,16	2,6,8,9,11,15	2^{-1}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,7,10	2,6,8,9,11,13	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,7,10,16,17,18	2,6,8,9,11,13,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,7,10,18	2,6,8,9,11,13,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,7,10,16,17	2,6,8,9,11,13,15,17	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,7,10,14,17,18	2,6,8,9,11,13,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,7,10,14,16	2,6,8,9,11,13	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,7,10,14,17	2,6,8,9,11,13,15,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,7,10,14,16,18	2,6,8,9,11,13,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,7,10,12,17	2,6,8,9,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,7,10,12,16,18	2,6,8,9,11,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,7,10,12,17,18	2,6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,7,10,12,16	2,6,8,9,11,15	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,7,10,12,14,18	2,6,8,9,11,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,7,10,12,14,16,17	2,6,8,9,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,7,10,12,14	2,6,8,9,11,15	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,7,10,12,14,16,17,18	2,6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,7,10,12,17,18	2,6,8,9,11,13,17,18	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,7,10,12,16	2,6,8,9,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,7,10,12,17	2,6,8,9,11,13,15,17	2^{-23}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,7,10,12,16,18	2,6,8,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,7,10,12,14	2,6,8,9,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,7,10,12,14,16,17,18	2,6,8,9,11,13,17,18	2^{-12}
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,7,10,12,14,18	2,6,8,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,7,10,12,14,16,17	2,6,8,9,11,13,15,17	2^{-12}

Table 0.1857 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,17	2,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,16,18	2,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,17,18	2,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,16	2,15	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,14,18	2,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,14,16,17	2,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,14	2,15	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,14,16,17,18	2,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,17,18	2,13,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,16	2,13	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,17	2,13,15,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,16,18	2,13,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,14	2,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,14,16,17,18	2,13,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,14,18	2,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,14,16,17	2,13,15,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,12,18	2,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,12,16,17	2,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,12	2,15	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,12,16,17,18	2,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,12,14,17	2,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,12,14,16,18	2,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,12,14,17,18	2,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,12,14,16	2,15	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,12	2,13	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,12,16,17,18	2,13,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,12,18	2,13,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,12,16,17	2,13,15,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,12,14,17,18	2,13,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,12,14,16	2,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,12,14,17	2,13,15,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,12,14,16,18	2,13,15,18	$2^{-17.5}$

Table 0.1858 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,17,18	2,11,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,16	2,11	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,17	2,11,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,16,18	2,11,15,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,14	2,11	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,14,16,17,18	2,11,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,14,18	2,11,15,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,14,16,17	2,11,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,17	2,11,13,17	2^{-1}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,16,18	2,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,17,18	2,11,13,15,17,18	2^{-1}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,16	2,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,14,18	2,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,14,16,17	2,11,13,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,14	2,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,14,16,17,18	2,11,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,12	2,11	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,12,16,17,18	2,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,12,18	2,11,15,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,12,16,17	2,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,12,14,17,18	2,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,12,14,16	2,11	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,12,14,17	2,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,12,14,16,18	2,11,15,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,12,18	2,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,12,16,17	2,11,13,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,12	2,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,12,16,17,18	2,11,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,12,14,17	2,11,13,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,12,14,16,18	2,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,12,14,17,18	2,11,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,12,14,16	2,11,13,15	$2^{-17.5}$

Table 0.1859 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,10,18	2,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,10,16,17	2,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,10	2,15	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,10,16,17,18	2,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,10,14,17	2,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,10,14,16,18	2,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,10,14,17,18	2,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,10,14,16	2,15	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,10	2,13	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,10,16,17,18	2,13,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,10,18	2,13,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,10,16,17	2,13,15,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,10,14,17,18	2,13,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,10,14,16	2,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,10,14,17	2,13,15,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,10,14,16,18	2,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,10,12,17	2,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,10,12,16,18	2,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,10,12,17,18	2,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,10,12,16	2,15	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,10,12,14,18	2,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,10,12,14,16,17	2,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,10,12,14	2,15	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,10,12,14,16,17,18	2,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,10,12,17,18	2,13,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,10,12,16	2,13	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,10,12,17	2,13,15,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,10,12,16,18	2,13,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,10,12,14	2,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,10,12,14,16,17,18	2,13,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,10,12,14,18	2,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,10,12,14,16,17	2,13,15,17	2^{-23}

Table 0.1860 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,10	2,11	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,10,16,17,18	2,11,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,10,18	2,11,15,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,10,16,17	2,11,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,10,14,17,18	2,11,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,10,14,16	2,11	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,10,14,17	2,11,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,10,14,16,18	2,11,15,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,10,18	2,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,10,16,17	2,11,13,17	2^{-34}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,10	2,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,10,16,17,18	2,11,13,15,17,18	2^{-34}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,10,14,17	2,11,13,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,10,14,16,18	2,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,10,14,17,18	2,11,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,10,14,16	2,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,10,12,17,18	2,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,10,12,16	2,11	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,10,12,17	2,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,10,12,16,18	2,11,15,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,10,12,14	2,11	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,10,12,14,16,17,18	2,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,10,12,14,18	2,11,15,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,10,12,14,16,17	2,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,10,12,17	2,11,13,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,10,12,16,18	2,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,10,12,17,18	2,11,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,10,12,16	2,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,10,12,14,18	2,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,10,12,14,16,17	2,11,13,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,10,12,14	2,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,10,12,14,16,17,18	2,11,13,15,17,18	2^{-23}

Table 0.1861 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,17,18	2,9,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,16	2,9	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,17	2,9,15,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,16,18	2,9,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,14	2,9	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,14,16,17,18	2,9,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,14,18	2,9,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,14,16,17	2,9,15,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,17	2,9,13,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,16,18	2,9,13,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,17,18	2,9,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,16	2,9,13,15	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,14,18	2,9,13,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,14,16,17	2,9,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,14	2,9,13,15	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,14,16,17,18	2,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,12	2,9	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,12,16,17,18	2,9,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,12,18	2,9,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,12,16,17	2,9,15,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,12,14,17,18	2,9,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,12,14,16	2,9	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,12,14,17	2,9,15,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,12,14,16,18	2,9,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,12,18	2,9,13,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,12,16,17	2,9,13,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,12	2,9,13,15	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,12,16,17,18	2,9,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,12,14,17	2,9,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,12,14,16,18	2,9,13,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,12,14,17,18	2,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,12,14,16	2,9,13,15	2^{-23}

Table 0.1862 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,17	2,9,11,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,16,18	2,9,11,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,17,18	2,9,11,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,16	2,9,11,15	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,14,18	2,9,11,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,14,16,17	2,9,11,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,14	2,9,11,15	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,14,16,17,18	2,9,11,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,17,18	2,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,16	2,9,11,13	2^{-34}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,17	2,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,16,18	2,9,11,13,15,18	2^{-34}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,14	2,9,11,13	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,14,16,17,18	2,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,14,18	2,9,11,13,15,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,14,16,17	2,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,12,18	2,9,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,12,16,17	2,9,11,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,12	2,9,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,12,16,17,18	2,9,11,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,12,14,17	2,9,11,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,12,14,16,18	2,9,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,12,14,17,18	2,9,11,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,12,14,16	2,9,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,12	2,9,11,13	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,12,16,17,18	2,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,12,18	2,9,11,13,15,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,12,16,17	2,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,12,14,17,18	2,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,12,14,16	2,9,11,13	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,12,14,17	2,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,12,14,16,18	2,9,11,13,15,18	2^{-23}

Table 0.1863 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,10	2,9	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,10,16,17,18	2,9,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,10,18	2,9,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,10,16,17	2,9,15,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,10,14,17,18	2,9,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,10,14,16	2,9	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,10,14,17	2,9,15,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,10,14,16,18	2,9,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,10,18	2,9,13,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,10,16,17	2,9,13,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,10	2,9,13,15	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,10,16,17,18	2,9,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,10,14,17	2,9,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,10,14,16,18	2,9,13,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,10,14,17,18	2,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,10,14,16	2,9,13,15	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,10,12,17,18	2,9,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,10,12,16	2,9	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,10,12,17	2,9,15,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,10,12,16,18	2,9,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,10,12,14	2,9	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,10,12,14,16,17,18	2,9,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,10,12,14,18	2,9,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,10,12,14,16,17	2,9,15,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,10,12,17	2,9,13,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,10,12,16,18	2,9,13,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,10,12,17,18	2,9,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,10,12,16	2,9,13,15	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,10,12,14,18	2,9,13,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,10,12,14,16,17	2,9,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,10,12,14	2,9,13,15	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,10,12,14,16,17,18	2,9,13,15,17,18	$2^{-17.5}$

Table 0.1864 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,10,18	2,9,11,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,10,16,17	2,9,11,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,10	2,9,11,15	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,10,16,17,18	2,9,11,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,10,14,17	2,9,11,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,10,14,16,18	2,9,11,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,10,14,17,18	2,9,11,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,10,14,16	2,9,11,15	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,10	2,9,11,13	2^{-1}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,10,16,17,18	2,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,10,18	2,9,11,13,15,18	2^{-1}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,10,16,17	2,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,10,14,17,18	2,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,10,14,16	2,9,11,13	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,10,14,17	2,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,10,14,16,18	2,9,11,13,15,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,10,12,17	2,9,11,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,10,12,16,18	2,9,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,10,12,17,18	2,9,11,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,10,12,16	2,9,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,10,12,14,18	2,9,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,10,12,14,16,17	2,9,11,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,10,12,14	2,9,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,10,12,14,16,17,18	2,9,11,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,10,12,17,18	2,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,10,12,16	2,9,11,13	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,10,12,17	2,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,10,12,16,18	2,9,11,13,15,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,10,12,14	2,9,11,13	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,10,12,14,16,17,18	2,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,10,12,14,18	2,9,11,13,15,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,10,12,14,16,17	2,9,11,13,15,17	$2^{-17.5}$

Table 0.1865 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,18	2,8,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,16,17	2,8,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,5	2,8,15	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,16,17,18	2,8,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,14,17	2,8,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,14,16,18	2,8,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,14,17,18	2,8,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,14,16	2,8,15	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,5	2,8,13	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,16,17,18	2,8,13,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,18	2,8,13,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,16,17	2,8,13,15,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,14,17,18	2,8,13,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,14,16	2,8,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,14,17	2,8,13,15,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,14,16,18	2,8,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,12,17	2,8,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,12,16,18	2,8,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,12,17,18	2,8,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,12,16	2,8,15	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,12,14,18	2,8,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,12,14,16,17	2,8,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,12,14	2,8,15	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,12,14,16,17,18	2,8,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,12,17,18	2,8,13,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,12,16	2,8,13	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,12,17	2,8,13,15,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,12,16,18	2,8,13,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,12,14	2,8,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,12,14,16,17,18	2,8,13,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,12,14,18	2,8,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,12,14,16,17	2,8,13,15,17	2^{-12}

Table 0.1866 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,5	2,8,11	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,16,17,18	2,8,11,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,18	2,8,11,15,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,16,17	2,8,11,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,14,17,18	2,8,11,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,14,16	2,8,11	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,14,17	2,8,11,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,14,16,18	2,8,11,15,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,18	2,8,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,16,17	2,8,11,13,17	2^{-1}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,5	2,8,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,16,17,18	2,8,11,13,15,17,18	2^{-1}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,14,17	2,8,11,13,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,14,16,18	2,8,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,14,17,18	2,8,11,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,14,16	2,8,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,12,17,18	2,8,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,12,16	2,8,11	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,12,17	2,8,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,12,16,18	2,8,11,15,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,12,14	2,8,11	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,12,14,16,17,18	2,8,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,12,14,18	2,8,11,15,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,12,14,16,17	2,8,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,12,17	2,8,11,13,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,12,16,18	2,8,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,12,17,18	2,8,11,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,12,16	2,8,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,12,14,18	2,8,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,12,14,16,17	2,8,11,13,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,12,14	2,8,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,12,14,16,17,18	2,8,11,13,15,17,18	2^{-12}

Table 0.1867 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,10,17	2,8,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,10,16,18	2,8,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,10,17,18	2,8,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,10,16	2,8,15	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,10,14,18	2,8,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,10,14,16,17	2,8,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,10,14	2,8,15	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,10,14,16,17,18	2,8,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,10,17,18	2,8,13,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,10,16	2,8,13	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,10,17	2,8,13,15,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,10,16,18	2,8,13,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,10,14	2,8,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,10,14,16,17,18	2,8,13,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,10,14,18	2,8,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,10,14,16,17	2,8,13,15,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,10,12,18	2,8,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,10,12,16,17	2,8,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,10,12	2,8,15	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,10,12,16,17,18	2,8,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,10,12,14,17	2,8,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,10,12,14,16,18	2,8,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,10,12,14,17,18	2,8,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,10,12,14,16	2,8,15	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,10,12	2,8,13	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,10,12,16,17,18	2,8,13,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,10,12,18	2,8,13,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,10,12,16,17	2,8,13,15,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,10,12,14,17,18	2,8,13,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,10,12,14,16	2,8,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,10,12,14,17	2,8,13,15,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,10,12,14,16,18	2,8,13,15,18	$2^{-17.5}$

Table 0.1868 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,10,17,18	2,8,11,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,10,16	2,8,11	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,10,17	2,8,11,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,10,16,18	2,8,11,15,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,10,14	2,8,11	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,10,14,16,17,18	2,8,11,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,10,14,18	2,8,11,15,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,10,14,16,17	2,8,11,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,10,17	2,8,11,13,17	2^{-34}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,10,16,18	2,8,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,10,17,18	2,8,11,13,15,17,18	2^{-34}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,10,16	2,8,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,10,14,18	2,8,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,10,14,16,17	2,8,11,13,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,10,14	2,8,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,10,14,16,17,18	2,8,11,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,10,12	2,8,11	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,10,12,16,17,18	2,8,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,10,12,18	2,8,11,15,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,10,12,16,17	2,8,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,10,12,14,17,18	2,8,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,10,12,14,16	2,8,11	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,10,12,14,17	2,8,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,10,12,14,16,18	2,8,11,15,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,10,12,18	2,8,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,10,12,16,17	2,8,11,13,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,10,12	2,8,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,10,12,16,17,18	2,8,11,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,10,12,14,17	2,8,11,13,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,10,12,14,16,18	2,8,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,10,12,14,17,18	2,8,11,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,10,12,14,16	2,8,11,13,15	$2^{-17.5}$

Table 0.1869 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,5	2,8,9	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,16,17,18	2,8,9,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,18	2,8,9,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,16,17	2,8,9,15,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,14,17,18	2,8,9,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,14,16	2,8,9	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,14,17	2,8,9,15,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,14,16,18	2,8,9,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,18	2,8,9,13,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,16,17	2,8,9,13,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,5	2,8,9,13,15	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,16,17,18	2,8,9,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,14,17	2,8,9,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,14,16,18	2,8,9,13,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,14,17,18	2,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,14,16	2,8,9,13,15	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,12,17,18	2,8,9,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,12,16	2,8,9	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,12,17	2,8,9,15,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,12,16,18	2,8,9,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,12,14	2,8,9	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,12,14,16,17,18	2,8,9,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,12,14,18	2,8,9,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,12,14,16,17	2,8,9,15,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,12,17	2,8,9,13,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,12,16,18	2,8,9,13,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,12,17,18	2,8,9,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,12,16	2,8,9,13,15	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,12,14,18	2,8,9,13,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,12,14,16,17	2,8,9,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,12,14	2,8,9,13,15	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,12,14,16,17,18	2,8,9,13,15,17,18	$2^{-17.5}$

Table 0.1870 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,18	2,8,9,11,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,16,17	2,8,9,11,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,5	2,8,9,11,15	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,16,17,18	2,8,9,11,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,14,17	2,8,9,11,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,14,16,18	2,8,9,11,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,14,17,18	2,8,9,11,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,14,16	2,8,9,11,15	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,5	2,8,9,11,13	2^{-34}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,16,17,18	2,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,18	2,8,9,11,13,15,18	2^{-34}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,16,17	2,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,14,17,18	2,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,14,16	2,8,9,11,13	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,14,17	2,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,14,16,18	2,8,9,11,13,15,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,12,17	2,8,9,11,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,12,16,18	2,8,9,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,12,17,18	2,8,9,11,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,12,16	2,8,9,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,12,14,18	2,8,9,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,12,14,16,17	2,8,9,11,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,12,14	2,8,9,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,12,14,16,17,18	2,8,9,11,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,12,17,18	2,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,12,16	2,8,9,11,13	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,12,17	2,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,12,16,18	2,8,9,11,13,15,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,12,14	2,8,9,11,13	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,12,14,16,17,18	2,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,12,14,18	2,8,9,11,13,15,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,12,14,16,17	2,8,9,11,13,15,17	$2^{-17.5}$

Table 0.1871 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,10,17,18	2,8,9,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,10,16	2,8,9	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,10,17	2,8,9,15,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,10,16,18	2,8,9,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,10,14	2,8,9	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,10,14,16,17,18	2,8,9,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,10,14,18	2,8,9,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,10,14,16,17	2,8,9,15,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,10,17	2,8,9,13,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,10,16,18	2,8,9,13,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,10,17,18	2,8,9,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,10,16	2,8,9,13,15	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,10,14,18	2,8,9,13,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,10,14,16,17	2,8,9,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,10,14	2,8,9,13,15	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,10,14,16,17,18	2,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,10,12	2,8,9	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,10,12,16,17,18	2,8,9,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,10,12,18	2,8,9,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,10,12,16,17	2,8,9,15,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,10,12,14,17,18	2,8,9,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,10,12,14,16	2,8,9	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,10,12,14,17	2,8,9,15,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,10,12,14,16,18	2,8,9,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,10,12,18	2,8,9,13,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,10,12,16,17	2,8,9,13,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,10,12	2,8,9,13,15	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,10,12,16,17,18	2,8,9,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,10,12,14,17	2,8,9,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,10,12,14,16,18	2,8,9,13,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,10,12,14,17,18	2,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,10,12,14,16	2,8,9,13,15	2^{-12}

Table 0.1872 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,10,17	2,8,9,11,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,10,16,18	2,8,9,11,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,10,17,18	2,8,9,11,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,10,16	2,8,9,11,15	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,10,14,18	2,8,9,11,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,10,14,16,17	2,8,9,11,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,10,14	2,8,9,11,15	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,10,14,16,17,18	2,8,9,11,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,10,17,18	2,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,10,16	2,8,9,11,13	2^{-1}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,10,17	2,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,10,16,18	2,8,9,11,13,15,18	2^{-1}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,10,14	2,8,9,11,13	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,10,14,16,17,18	2,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,10,14,18	2,8,9,11,13,15,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,10,14,16,17	2,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,10,12,18	2,8,9,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,10,12,16,17	2,8,9,11,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,10,12	2,8,9,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,10,12,16,17,18	2,8,9,11,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,10,12,14,17	2,8,9,11,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,10,12,14,16,18	2,8,9,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,10,12,14,17,18	2,8,9,11,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,10,12,14,16	2,8,9,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,10,12	2,8,9,11,13	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,10,12,16,17,18	2,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,10,12,18	2,8,9,11,13,15,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,10,12,16,17	2,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,10,12,14,17,18	2,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,10,12,14,16	2,8,9,11,13	2^{-12}
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,10,12,14,17	2,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,10,12,14,16,18	2,8,9,11,13,15,18	2^{-12}

Table 0.1873 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,17,18	2,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,7,16	2	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,17	2,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,7,16,18	2,15,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,7,14	2	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,14,16,17,18	2,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,7,14,18	2,15,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,14,16,17	2,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,7,17	2,13,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,7,16,18	2,13,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,7,17,18	2,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,7,16	2,13,15	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,7,14,18	2,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,7,14,16,17	2,13,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,7,14	2,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,7,14,16,17,18	2,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,7,12	2	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,7,12,16,17,18	2,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,7,12,18	2,15,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,7,12,16,17	2,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,7,12,14,17,18	2,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,7,12,14,16	2	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,7,12,14,17	2,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,7,12,14,16,18	2,15,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,7,12,18	2,13,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,7,12,16,17	2,13,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,7,12	2,13,15	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,7,12,16,17,18	2,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,7,12,14,17	2,13,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,7,12,14,16,18	2,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,7,12,14,17,18	2,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,7,12,14,16	2,13,15	$2^{-17.5}$

Table 0.1874 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,7,17	2,11,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,7,16,18	2,11,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,7,17,18	2,11,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,7,16	2,11,15	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,7,14,18	2,11,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,7,14,16,17	2,11,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,7,14	2,11,15	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,7,14,16,17,18	2,11,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,7,17,18	2,11,13,17,18	2^{-1}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,7,16	2,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,7,17	2,11,13,15,17	2^{-1}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,7,16,18	2,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,14	2,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,7,14,16,17,18	2,11,13,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,14,18	2,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,7,14,16,17	2,11,13,15,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,7,12,18	2,11,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,7,12,16,17	2,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,7,12	2,11,15	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,7,12,16,17,18	2,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,7,12,14,17	2,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,7,12,14,16,18	2,11,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,7,12,14,17,18	2,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,7,12,14,16	2,11,15	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,7,12	2,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,7,12,16,17,18	2,11,13,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,7,12,18	2,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,7,12,16,17	2,11,13,15,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,7,12,14,17,18	2,11,13,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,7,12,14,16	2,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,7,12,14,17	2,11,13,15,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,7,12,14,16,18	2,11,13,15,18	$2^{-17.5}$

Table 0.1875 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,7,10	2	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,7,10,16,17,18	2,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,7,10,18	2,15,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,7,10,16,17	2,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,7,10,14,17,18	2,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,7,10,14,16	2	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,7,10,14,17	2,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,7,10,14,16,18	2,15,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,7,10,18	2,13,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,7,10,16,17	2,13,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,7,10	2,13,15	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,7,10,16,17,18	2,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,7,10,14,17	2,13,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,7,10,14,16,18	2,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,7,10,14,17,18	2,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,7,10,14,16	2,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,7,10,12,17,18	2,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,7,10,12,16	2	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,7,10,12,17	2,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,7,10,12,16,18	2,15,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,7,10,12,14	2	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,7,10,12,14,16,17,18	2,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,7,10,12,14,18	2,15,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,7,10,12,14,16,17	2,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,7,10,12,17	2,13,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,7,10,12,16,18	2,13,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,7,10,12,17,18	2,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,7,10,12,16	2,13,15	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,7,10,12,14,18	2,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,7,10,12,14,16,17	2,13,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,7,10,12,14	2,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,7,10,12,14,16,17,18	2,13,15,17,18	2^{-23}

Table 0.1876 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,7,10,18	2,11,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,7,10,16,17	2,11,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,7,10	2,11,15	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,7,10,16,17,18	2,11,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,7,10,14,17	2,11,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,7,10,14,16,18	2,11,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,7,10,14,17,18	2,11,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,7,10,14,16	2,11,15	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,7,10	2,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,7,10,16,17,18	2,11,13,17,18	2^{-34}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,7,10,18	2,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,7,10,16,17	2,11,13,15,17	2^{-34}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,7,10,14,17,18	2,11,13,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,7,10,14,16	2,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,7,10,14,17	2,11,13,15,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,7,10,14,16,18	2,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,7,10,12,17	2,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,7,10,12,16,18	2,11,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,7,10,12,17,18	2,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,7,10,12,16	2,11,15	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,7,10,12,14,18	2,11,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,7,10,12,14,16,17	2,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,7,10,12,14	2,11,15	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,7,10,12,14,16,17,18	2,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,7,10,12,17,18	2,11,13,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,7,10,12,16	2,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,7,10,12,17	2,11,13,15,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,7,10,12,16,18	2,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,7,10,12,14	2,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7,10,12,14,16,17,18	2,11,13,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,7,10,12,14,18	2,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,7,10,12,14,16,17	2,11,13,15,17	2^{-23}

Table 0.1877 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,7,17	2,9,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,7,16,18	2,9,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,7,17,18	2,9,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,7,16	2,9,15	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,7,14,18	2,9,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,7,14,16,17	2,9,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,7,14	2,9,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,7,14,16,17,18	2,9,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,7,17,18	2,9,13,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,7,16	2,9,13	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,7,17	2,9,13,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,7,16,18	2,9,13,15,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,7,14	2,9,13	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,7,14,16,17,18	2,9,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,7,14,18	2,9,13,15,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,7,14,16,17	2,9,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,7,12,18	2,9,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,7,12,16,17	2,9,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,7,12	2,9,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,7,12,16,17,18	2,9,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,7,12,14,17	2,9,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,7,12,14,16,18	2,9,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,7,12,14,17,18	2,9,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,7,12,14,16	2,9,15	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,7,12	2,9,13	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,7,12,16,17,18	2,9,13,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,7,12,18	2,9,13,15,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,7,12,16,17	2,9,13,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,7,12,14,17,18	2,9,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,7,12,14,16	2,9,13	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,7,12,14,17	2,9,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,7,12,14,16,18	2,9,13,15,18	2^{-23}

Table 0.1878 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,7,17,18	2,9,11,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,7,16	2,9,11	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,7,17	2,9,11,15,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,7,16,18	2,9,11,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,7,14	2,9,11	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,7,14,16,17,18	2,9,11,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,7,14,18	2,9,11,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,7,14,16,17	2,9,11,15,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,7,17	2,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,7,16,18	2,9,11,13,18	2^{-34}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,7,17,18	2,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,7,16	2,9,11,13,15	2^{-34}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,7,14,18	2,9,11,13,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,7,14,16,17	2,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,7,14	2,9,11,13,15	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,7,14,16,17,18	2,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,7,12	2,9,11	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,7,12,16,17,18	2,9,11,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,7,12,18	2,9,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,7,12,16,17	2,9,11,15,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,7,12,14,17,18	2,9,11,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,7,12,14,16	2,9,11	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,7,12,14,17	2,9,11,15,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,7,12,14,16,18	2,9,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,7,12,18	2,9,11,13,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,7,12,16,17	2,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,7,12	2,9,11,13,15	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,7,12,16,17,18	2,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,7,12,14,17	2,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,7,12,14,16,18	2,9,11,13,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,7,12,14,17,18	2,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,7,12,14,16	2,9,11,13,15	2^{-23}

Table 0.1879 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,7,10,18	2,9,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,7,10,16,17	2,9,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,7,10	2,9,15	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,7,10,16,17,18	2,9,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,7,10,14,17	2,9,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,7,10,14,16,18	2,9,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,7,10,14,17,18	2,9,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,7,10,14,16	2,9,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,7,10	2,9,13	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,7,10,16,17,18	2,9,13,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,7,10,18	2,9,13,15,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,7,10,16,17	2,9,13,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,7,10,14,17,18	2,9,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,7,10,14,16	2,9,13	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,7,10,14,17	2,9,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,7,10,14,16,18	2,9,13,15,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,7,10,12,17	2,9,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,7,10,12,16,18	2,9,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,7,10,12,17,18	2,9,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,7,10,12,16	2,9,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10,12,14,18	2,9,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,12,14,16,17	2,9,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10,12,14	2,9,15	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,12,14,16,17,18	2,9,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,7,10,12,17,18	2,9,13,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,7,10,12,16	2,9,13	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,7,10,12,17	2,9,13,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,7,10,12,16,18	2,9,13,15,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10,12,14	2,9,13	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,12,14,16,17,18	2,9,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10,12,14,18	2,9,13,15,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,12,14,16,17	2,9,13,15,17	$2^{-17.5}$

Table 0.1880 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,7,10	2,9,11	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,7,10,16,17,18	2,9,11,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,7,10,18	2,9,11,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,7,10,16,17	2,9,11,15,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,7,10,14,17,18	2,9,11,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,7,10,14,16	2,9,11	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,7,10,14,17	2,9,11,15,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,7,10,14,16,18	2,9,11,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,7,10,18	2,9,11,13,18	2^{-1}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,7,10,16,17	2,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,7,10	2,9,11,13,15	2^{-1}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,7,10,16,17,18	2,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,7,10,14,17	2,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,7,10,14,16,18	2,9,11,13,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,7,10,14,17,18	2,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,7,10,14,16	2,9,11,13,15	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,7,10,12,17,18	2,9,11,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,7,10,12,16	2,9,11	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,7,10,12,17	2,9,11,15,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,7,10,12,16,18	2,9,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,7,10,12,14	2,9,11	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7,10,12,14,16,17,18	2,9,11,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,7,10,12,14,18	2,9,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7,10,12,14,16,17	2,9,11,15,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,7,10,12,17	2,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,7,10,12,16,18	2,9,11,13,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,7,10,12,17,18	2,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,7,10,12,16	2,9,11,13,15	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,7,10,12,14,18	2,9,11,13,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,7,10,12,14,16,17	2,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,7,10,12,14	2,9,11,13,15	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,7,10,12,14,16,17,18	2,9,11,13,15,17,18	$2^{-17.5}$

Table 0.1881 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,7	2,8	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,7,16,17,18	2,8,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,7,18	2,8,15,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,7,16,17	2,8,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,7,14,17,18	2,8,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,7,14,16	2,8	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,7,14,17	2,8,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,7,14,16,18	2,8,15,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,7,18	2,8,13,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,7,16,17	2,8,13,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,7	2,8,13,15	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,7,16,17,18	2,8,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,7,14,17	2,8,13,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,7,14,16,18	2,8,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,7,14,17,18	2,8,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,7,14,16	2,8,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,7,12,17,18	2,8,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,7,12,16	2,8	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,7,12,17	2,8,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,7,12,16,18	2,8,15,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,7,12,14	2,8	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,7,12,14,16,17,18	2,8,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,7,12,14,18	2,8,15,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,7,12,14,16,17	2,8,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,7,12,17	2,8,13,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,7,12,16,18	2,8,13,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,7,12,17,18	2,8,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,7,12,16	2,8,13,15	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,7,12,14,18	2,8,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,7,12,14,16,17	2,8,13,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,7,12,14	2,8,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,7,12,14,16,17,18	2,8,13,15,17,18	2^{-12}

Table 0.1882 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,7,18	2,8,11,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,7,16,17	2,8,11,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,7	2,8,11,15	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,7,16,17,18	2,8,11,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,7,14,17	2,8,11,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,7,14,16,18	2,8,11,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,7,14,17,18	2,8,11,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,7,14,16	2,8,11,15	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,7	2,8,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,7,16,17,18	2,8,11,13,17,18	2^{-1}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,7,18	2,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,7,16,17	2,8,11,13,15,17	2^{-1}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,7,14,17,18	2,8,11,13,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,7,14,16	2,8,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,7,14,17	2,8,11,13,15,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,7,14,16,18	2,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,7,12,17	2,8,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,7,12,16,18	2,8,11,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,7,12,17,18	2,8,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,7,12,16	2,8,11,15	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7,12,14,18	2,8,11,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,7,12,14,16,17	2,8,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7,12,14	2,8,11,15	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,7,12,14,16,17,18	2,8,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,7,12,17,18	2,8,11,13,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,7,12,16	2,8,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,7,12,17	2,8,11,13,15,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,7,12,16,18	2,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,7,12,14	2,8,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,7,12,14,16,17,18	2,8,11,13,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,7,12,14,18	2,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,7,12,14,16,17	2,8,11,13,15,17	2^{-12}

Table 0.1883 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,7,10,17,18	2,8,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,7,10,16	2,8	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,7,10,17	2,8,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,7,10,16,18	2,8,15,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,7,10,14	2,8	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,7,10,14,16,17,18	2,8,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,7,10,14,18	2,8,15,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,7,10,14,16,17	2,8,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,7,10,17	2,8,13,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,7,10,16,18	2,8,13,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,7,10,17,18	2,8,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,7,10,16	2,8,13,15	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,7,10,14,18	2,8,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,7,10,14,16,17	2,8,13,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,7,10,14	2,8,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,7,10,14,16,17,18	2,8,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,7,10,12	2,8	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,7,10,12,16,17,18	2,8,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,7,10,12,18	2,8,15,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,7,10,12,16,17	2,8,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,7,10,12,14,17,18	2,8,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,7,10,12,14,16	2,8	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,7,10,12,14,17	2,8,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,7,10,12,14,16,18	2,8,15,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,7,10,12,18	2,8,13,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,7,10,12,16,17	2,8,13,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,7,10,12	2,8,13,15	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,7,10,12,16,17,18	2,8,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,7,10,12,14,17	2,8,13,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,7,10,12,14,16,18	2,8,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,7,10,12,14,17,18	2,8,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,7,10,12,14,16	2,8,13,15	$2^{-17.5}$

Table 0.1884 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,7,10,17	2,8,11,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,7,10,16,18	2,8,11,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,7,10,17,18	2,8,11,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,7,10,16	2,8,11,15	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,7,10,14,18	2,8,11,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,7,10,14,16,17	2,8,11,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,7,10,14	2,8,11,15	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,7,10,14,16,17,18	2,8,11,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,7,10,17,18	2,8,11,13,17,18	2^{-34}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,7,10,16	2,8,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,7,10,17	2,8,11,13,15,17	2^{-34}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,7,10,16,18	2,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,7,10,14	2,8,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,7,10,14,16,17,18	2,8,11,13,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,7,10,14,18	2,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,7,10,14,16,17	2,8,11,13,15,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,7,10,12,18	2,8,11,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,7,10,12,16,17	2,8,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,7,10,12	2,8,11,15	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,7,10,12,16,17,18	2,8,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,7,10,12,14,17	2,8,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,7,10,12,14,16,18	2,8,11,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,7,10,12,14,17,18	2,8,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,7,10,12,14,16	2,8,11,15	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,7,10,12	2,8,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,7,10,12,16,17,18	2,8,11,13,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,7,10,12,18	2,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,7,10,12,16,17	2,8,11,13,15,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,7,10,12,14,17,18	2,8,11,13,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,7,10,12,14,16	2,8,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,7,10,12,14,17	2,8,11,13,15,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,7,10,12,14,16,18	2,8,11,13,15,18	$2^{-17.5}$

Table 0.1885 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,7,18	2,8,9,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,7,16,17	2,8,9,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7	2,8,9,15	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,7,16,17,18	2,8,9,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,7,14,17	2,8,9,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,7,14,16,18	2,8,9,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,7,14,17,18	2,8,9,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,7,14,16	2,8,9,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,7	2,8,9,13	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,7,16,17,18	2,8,9,13,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,7,18	2,8,9,13,15,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,7,16,17	2,8,9,13,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,7,14,17,18	2,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,7,14,16	2,8,9,13	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,7,14,17	2,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,7,14,16,18	2,8,9,13,15,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,7,12,17	2,8,9,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,7,12,16,18	2,8,9,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,7,12,17,18	2,8,9,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,7,12,16	2,8,9,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,7,12,14,18	2,8,9,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,7,12,14,16,17	2,8,9,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,7,12,14	2,8,9,15	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,7,12,14,16,17,18	2,8,9,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,7,12,17,18	2,8,9,13,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,7,12,16	2,8,9,13	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,7,12,17	2,8,9,13,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,7,12,16,18	2,8,9,13,15,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,7,12,14	2,8,9,13	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,7,12,14,16,17,18	2,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,7,12,14,18	2,8,9,13,15,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,7,12,14,16,17	2,8,9,13,15,17	$2^{-17.5}$

Table 0.1886 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,7	2,8,9,11	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,7,16,17,18	2,8,9,11,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,7,18	2,8,9,11,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,7,16,17	2,8,9,11,15,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,7,14,17,18	2,8,9,11,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,7,14,16	2,8,9,11	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,7,14,17	2,8,9,11,15,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,7,14,16,18	2,8,9,11,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,7,18	2,8,9,11,13,18	2^{-34}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,7,16,17	2,8,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,7	2,8,9,11,13,15	2^{-34}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,7,16,17,18	2,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,7,14,17	2,8,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,7,14,16,18	2,8,9,11,13,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,7,14,17,18	2,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,7,14,16	2,8,9,11,13,15	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,7,12,17,18	2,8,9,11,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,7,12,16	2,8,9,11	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,7,12,17	2,8,9,11,15,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,7,12,16,18	2,8,9,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,7,12,14	2,8,9,11	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,7,12,14,16,17,18	2,8,9,11,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,7,12,14,18	2,8,9,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,7,12,14,16,17	2,8,9,11,15,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,7,12,17	2,8,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,7,12,16,18	2,8,9,11,13,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,7,12,17,18	2,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,7,12,16	2,8,9,11,13,15	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7,12,14,18	2,8,9,11,13,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,7,12,14,16,17	2,8,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7,12,14	2,8,9,11,13,15	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,7,12,14,16,17,18	2,8,9,11,13,15,17,18	$2^{-17.5}$

Table 0.1887 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,7,10,17	2,8,9,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,10,16,18	2,8,9,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,7,10,17,18	2,8,9,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,10,16	2,8,9,15	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,10,14,18	2,8,9,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,7,10,14,16,17	2,8,9,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,10,14	2,8,9,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,7,10,14,16,17,18	2,8,9,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,7,10,17,18	2,8,9,13,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,7,10,16	2,8,9,13	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,7,10,17	2,8,9,13,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,7,10,16,18	2,8,9,13,15,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,7,10,14	2,8,9,13	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,7,10,14,16,17,18	2,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,7,10,14,18	2,8,9,13,15,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,7,10,14,16,17	2,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,7,10,12,18	2,8,9,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,12,16,17	2,8,9,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,7,10,12	2,8,9,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,12,16,17,18	2,8,9,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,7,10,12,14,17	2,8,9,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,7,10,12,14,16,18	2,8,9,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,7,10,12,14,17,18	2,8,9,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,7,10,12,14,16	2,8,9,15	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,7,10,12	2,8,9,13	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,12,16,17,18	2,8,9,13,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,7,10,12,18	2,8,9,13,15,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,12,16,17	2,8,9,13,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,7,10,12,14,17,18	2,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,7,10,12,14,16	2,8,9,13	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,7,10,12,14,17	2,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,7,10,12,14,16,18	2,8,9,13,15,18	2^{-12}

Table 0.1888 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,7,10,17,18	2,8,9,11,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,7,10,16	2,8,9,11	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,7,10,17	2,8,9,11,15,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,7,10,16,18	2,8,9,11,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,7,10,14	2,8,9,11	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,7,10,14,16,17,18	2,8,9,11,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,7,10,14,18	2,8,9,11,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,7,10,14,16,17	2,8,9,11,15,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,7,10,17	2,8,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,7,10,16,18	2,8,9,11,13,18	2^{-1}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,7,10,17,18	2,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,7,10,16	2,8,9,11,13,15	2^{-1}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,7,10,14,18	2,8,9,11,13,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,10,14,16,17	2,8,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,7,10,14	2,8,9,11,13,15	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,10,14,16,17,18	2,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,7,10,12	2,8,9,11	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,7,10,12,16,17,18	2,8,9,11,17,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,7,10,12,18	2,8,9,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,7,10,12,16,17	2,8,9,11,15,17	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,7,10,12,14,17,18	2,8,9,11,17,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,7,10,12,14,16	2,8,9,11	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,7,10,12,14,17	2,8,9,11,15,17	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,7,10,12,14,16,18	2,8,9,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,7,10,12,18	2,8,9,11,13,18	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,7,10,12,16,17	2,8,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,7,10,12	2,8,9,11,13,15	2^{-23}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,7,10,12,16,17,18	2,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,7,10,12,14,17	2,8,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,7,10,12,14,16,18	2,8,9,11,13,18	2^{-12}
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,7,10,12,14,17,18	2,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,7,10,12,14,16	2,8,9,11,13,15	2^{-12}

Table 0.1889 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,18	2,6,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,16,17	2,6,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,5	2,6,15	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,16,17,18	2,6,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,14,17	2,6,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,14,16,18	2,6,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,14,17,18	2,6,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,14,16	2,6,15	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,5	2,6,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,16,17,18	2,6,13,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,18	2,6,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,16,17	2,6,13,15,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,14,17,18	2,6,13,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,14,16	2,6,13	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,14,17	2,6,13,15,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,14,16,18	2,6,13,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,12,17	2,6,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,12,16,18	2,6,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,12,17,18	2,6,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,12,16	2,6,15	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,12,14,18	2,6,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,12,17,18	2,6,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,12,14,16,17	2,6,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,12,14	2,6,15	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,12,14,16,17,18	2,6,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,12,17,18	2,6,13,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,12,16	2,6,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,12,17	2,6,13,15,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,12,16,18	2,6,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,12,14	2,6,13	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,12,14,16,17,18	2,6,13,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,12,14,18	2,6,13,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,12,14,16,17	2,6,13,15,17	2^{-12}

Table 0.1890 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,5	2,6,11	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,16,17,18	2,6,11,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,18	2,6,11,15,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,16,17	2,6,11,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,14,17,18	2,6,11,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,14,16	2,6,11	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,14,17	2,6,11,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,14,16,18	2,6,11,15,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,18	2,6,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,16,17	2,6,11,13,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,5	2,6,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,16,17,18	2,6,11,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,14,17	2,6,11,13,17	2^{-1}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,14,16,18	2,6,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,14,17,18	2,6,11,13,15,17,18	2^{-1}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,14,16	2,6,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,12,17,18	2,6,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,12,16	2,6,11	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,12,17	2,6,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,12,16,18	2,6,11,15,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,12,14	2,6,11	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,12,14,16,17,18	2,6,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,12,14,18	2,6,11,15,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,12,14,16,17	2,6,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,12,17	2,6,11,13,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,12,16,18	2,6,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,12,17,18	2,6,11,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,12,16	2,6,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,12,14,18	2,6,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,12,14,16,17	2,6,11,13,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,12,14	2,6,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,12,14,16,17,18	2,6,11,13,15,17,18	2^{-23}

Table 0.1891 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,10,17	2,6,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,10,16,18	2,6,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,10,17,18	2,6,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,10,16	2,6,15	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,10,14,18	2,6,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,10,14,16,17	2,6,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,10,14	2,6,15	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,10,14,16,17,18	2,6,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,10,17,18	2,6,13,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,10,16	2,6,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,10,17	2,6,13,15,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,10,16,18	2,6,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,10,14	2,6,13	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,10,14,16,17,18	2,6,13,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,10,14,18	2,6,13,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,10,14,16,17	2,6,13,15,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,10,12,18	2,6,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,10,12,16,17	2,6,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,10,12	2,6,15	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,10,12,16,17,18	2,6,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,10,12,14,17	2,6,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,10,12,14,16,18	2,6,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,10,12,14,17,18	2,6,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,10,12,14,16	2,6,15	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,10,12	2,6,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,10,12,16,17,18	2,6,13,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,10,12,18	2,6,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,10,12,16,17	2,6,13,15,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,10,12,14,17,18	2,6,13,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,10,12,14,16	2,6,13	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,10,12,14,17	2,6,13,15,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,10,12,14,16,18	2,6,13,15,18	$2^{-28.5}$

Table 0.1892 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,10,17,18	2,6,11,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,10,16	2,6,11	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,10,17	2,6,11,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,10,16,18	2,6,11,15,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,10,14	2,6,11	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,10,14,16,17,18	2,6,11,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,10,14,18	2,6,11,15,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,10,14,16,17	2,6,11,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,10,17	2,6,11,13,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,10,16,18	2,6,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,10,17,18	2,6,11,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,10,16	2,6,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,10,14,18	2,6,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,10,14,16,17	2,6,11,13,17	2^{-34}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,10,14	2,6,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,10,14,16,17,18	2,6,11,13,15,17,18	2^{-34}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,10,12	2,6,11	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,10,12,16,17,18	2,6,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,10,12,18	2,6,11,15,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,10,12,16,17	2,6,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,10,12,14,17,18	2,6,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,10,12,14,16	2,6,11	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,10,12,14,17	2,6,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,10,12,14,16,18	2,6,11,15,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,10,12,18	2,6,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,10,12,16,17	2,6,11,13,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,10,12	2,6,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,10,12,16,17,18	2,6,11,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,10,12,14,17	2,6,11,13,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,10,12,14,16,18	2,6,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,10,12,14,17,18	2,6,11,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,10,12,14,16	2,6,11,13,15	$2^{-17.5}$

Table 0.1893 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,5	2,6,9	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,16,17,18	2,6,9,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,18	2,6,9,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,16,17	2,6,9,15,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,14,17,18	2,6,9,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,14,16	2,6,9	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,14,17	2,6,9,15,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,14,16,18	2,6,9,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,18	2,6,9,13,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,16,17	2,6,9,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,5	2,6,9,13,15	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,16,17,18	2,6,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,14,17	2,6,9,13,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,14,16,18	2,6,9,13,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,14,17,18	2,6,9,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,14,16	2,6,9,13,15	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,12,17,18	2,6,9,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,12,16	2,6,9	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,12,17	2,6,9,15,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,12,16,18	2,6,9,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,12,14	2,6,9	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,12,14,16,17,18	2,6,9,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,12,14,18	2,6,9,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,12,14,16,17	2,6,9,15,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,12,17	2,6,9,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,12,16,18	2,6,9,13,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,12,17,18	2,6,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,12,16	2,6,9,13,15	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,12,14,18	2,6,9,13,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,12,14,16,17	2,6,9,13,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,12,14	2,6,9,13,15	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,12,14,16,17,18	2,6,9,13,15,17,18	$2^{-28.5}$

Table 0.1894 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,18	2,6,9,11,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,16,17	2,6,9,11,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,5	2,6,9,11,15	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,16,17,18	2,6,9,11,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,14,17	2,6,9,11,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,14,16,18	2,6,9,11,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,14,17,18	2,6,9,11,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,14,16	2,6,9,11,15	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,5	2,6,9,11,13	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,16,17,18	2,6,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,18	2,6,9,11,13,15,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,16,17	2,6,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,14,17,18	2,6,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,14,16	2,6,9,11,13	2^{-34}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,14,17	2,6,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,14,16,18	2,6,9,11,13,15,18	2^{-34}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,12,17	2,6,9,11,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,12,16,18	2,6,9,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,12,17,18	2,6,9,11,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,12,16	2,6,9,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,12,14,18	2,6,9,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,12,14,16,17	2,6,9,11,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,12,14	2,6,9,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,12,14,16,17,18	2,6,9,11,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,12,17,18	2,6,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,12,16	2,6,9,11,13	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,12,17	2,6,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,12,16,18	2,6,9,11,13,15,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,12,14	2,6,9,11,13	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,12,14,16,17,18	2,6,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,12,14,18	2,6,9,11,13,15,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,12,14,16,17	2,6,9,11,13,15,17	$2^{-17.5}$

Table 0.1895 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,10,17,18	2,6,9,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,10,16	2,6,9	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,10,17	2,6,9,15,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,10,16,18	2,6,9,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,10,14	2,6,9	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,10,14,16,17,18	2,6,9,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,10,14,18	2,6,9,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,10,14,16,17	2,6,9,15,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,10,17	2,6,9,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,10,16,18	2,6,9,13,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,10,17,18	2,6,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,10,16	2,6,9,13,15	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,10,14,18	2,6,9,13,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,10,14,16,17	2,6,9,13,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,10,14	2,6,9,13,15	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,10,14,16,17,18	2,6,9,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,10,12	2,6,9	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,10,12,16,17,18	2,6,9,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,10,12,18	2,6,9,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,10,12,16,17	2,6,9,15,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,10,12,14,17,18	2,6,9,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,10,12,14,16	2,6,9	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,10,12,14,17	2,6,9,15,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,10,12,14,16,18	2,6,9,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,10,12,18	2,6,9,13,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,10,12,16,17	2,6,9,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,10,12	2,6,9,13,15	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,10,12,16,17,18	2,6,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,10,12,14,17	2,6,9,13,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,10,12,14,16,18	2,6,9,13,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,10,12,14,17,18	2,6,9,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,10,12,14,16	2,6,9,13,15	2^{-12}

Table 0.1896 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,10,17	2,6,9,11,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,10,16,18	2,6,9,11,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,10,17,18	2,6,9,11,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,10,16	2,6,9,11,15	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,10,14,18	2,6,9,11,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,10,14,16,17	2,6,9,11,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,10,14	2,6,9,11,15	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,10,14,16,17,18	2,6,9,11,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,10,17,18	2,6,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,10,16	2,6,9,11,13	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,10,17	2,6,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,10,16,18	2,6,9,11,13,15,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,10,14	2,6,9,11,13	2^{-1}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,10,14,16,17,18	2,6,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,10,14,18	2,6,9,11,13,15,18	2^{-1}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,10,14,16,17	2,6,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,10,12,18	2,6,9,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,10,12,16,17	2,6,9,11,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,10,12	2,6,9,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,10,12,16,17,18	2,6,9,11,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,10,12,14,17	2,6,9,11,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,10,12,14,16,18	2,6,9,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,10,12,14,17,18	2,6,9,11,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,10,12,14,16	2,6,9,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,10,12	2,6,9,11,13	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,10,12,16,17,18	2,6,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,10,12,18	2,6,9,11,13,15,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,10,12,16,17	2,6,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,10,12,14,17,18	2,6,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,10,12,14,16	2,6,9,11,13	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,10,12,14,17	2,6,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,10,12,14,16,18	2,6,9,11,13,15,18	2^{-23}

Table 0.1897 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,17	2,6,8,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,16,18	2,6,8,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,17,18	2,6,8,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,16	2,6,8,15	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,14,18	2,6,8,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,14,16,17	2,6,8,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,14	2,6,8,15	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,14,16,17,18	2,6,8,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,17,18	2,6,8,13,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,16	2,6,8,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,17	2,6,8,13,15,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,16,18	2,6,8,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,14	2,6,8,13	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,14,16,17,18	2,6,8,13,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,14,18	2,6,8,13,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,14,16,17	2,6,8,13,15,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,12,18	2,6,8,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,12,16,17	2,6,8,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,12	2,6,8,15	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,12,16,17,18	2,6,8,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,12,14,17	2,6,8,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,12,14,16,18	2,6,8,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,12,14,17,18	2,6,8,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,12,14,16	2,6,8,15	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,12	2,6,8,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,12,16,17,18	2,6,8,13,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,12,18	2,6,8,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,12,16,17	2,6,8,13,15,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,12,14,17,18	2,6,8,13,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,12,14,16	2,6,8,13	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,12,14,17	2,6,8,13,15,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,12,14,16,18	2,6,8,13,15,18	$2^{-6.5}$

Table 0.1898 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,17,18	2,6,8,11,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,16	2,6,8,11	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,17	2,6,8,11,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,16,18	2,6,8,11,15,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,14	2,6,8,11	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,14,16,17,18	2,6,8,11,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,14,18	2,6,8,11,15,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,14,16,17	2,6,8,11,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,17	2,6,8,11,13,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,16,18	2,6,8,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,17,18	2,6,8,11,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,16	2,6,8,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,14,18	2,6,8,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,14,16,17	2,6,8,11,13,17	2^{-1}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,14	2,6,8,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,14,16,17,18	2,6,8,11,13,15,17,18	2^{-1}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,12	2,6,8,11	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,12,16,17,18	2,6,8,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,12,18	2,6,8,11,15,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,12,16,17	2,6,8,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,12,14,17,18	2,6,8,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,12,14,16	2,6,8,11	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,12,14,17	2,6,8,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,12,14,16,18	2,6,8,11,15,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,12,18	2,6,8,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,12,16,17	2,6,8,11,13,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,12	2,6,8,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,12,16,17,18	2,6,8,11,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,12,14,17	2,6,8,11,13,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,12,14,16,18	2,6,8,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,12,14,17,18	2,6,8,11,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,12,14,16	2,6,8,11,13,15	$2^{-17.5}$

Table 0.1899 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,10,18	2,6,8,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,10,16,17	2,6,8,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,10	2,6,8,15	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,10,16,17,18	2,6,8,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,10,14,17	2,6,8,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,10,14,16,18	2,6,8,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,10,14,17,18	2,6,8,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,10,14,16	2,6,8,15	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,10	2,6,8,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,10,16,17,18	2,6,8,13,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,10,18	2,6,8,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,10,16,17	2,6,8,13,15,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,10,14,17,18	2,6,8,13,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,10,14,16	2,6,8,13	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,10,14,17	2,6,8,13,15,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,10,14,16,18	2,6,8,13,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,10,12,17	2,6,8,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,10,12,16,18	2,6,8,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,10,12,17,18	2,6,8,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,10,12,16	2,6,8,15	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,10,12,14,18	2,6,8,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,10,12,17,18	2,6,8,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,10,12,14,16,17	2,6,8,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,10,12,14	2,6,8,15	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,10,12,14,16,17,18	2,6,8,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,10,12,17,18	2,6,8,13,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,10,12,16	2,6,8,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,10,12,17	2,6,8,13,15,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,10,12,16,18	2,6,8,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,10,12,14	2,6,8,13	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,10,12,14,16,17,18	2,6,8,13,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,10,12,14,18	2,6,8,13,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,10,12,14,16,17	2,6,8,13,15,17	2^{-23}

Table 0.1900 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,10	2,6,8,11	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,10,16,17,18	2,6,8,11,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,10,18	2,6,8,11,15,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,10,16,17	2,6,8,11,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,10,14,17,18	2,6,8,11,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,10,14,16	2,6,8,11	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,10,14,17	2,6,8,11,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,10,14,16,18	2,6,8,11,15,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,10,18	2,6,8,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,10,16,17	2,6,8,11,13,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,10	2,6,8,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,10,16,17,18	2,6,8,11,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,10,14,17	2,6,8,11,13,17	2^{-34}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,10,14,16,18	2,6,8,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,10,14,17,18	2,6,8,11,13,15,17,18	2^{-34}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,10,14,16	2,6,8,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,10,12,17,18	2,6,8,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,10,12,16	2,6,8,11	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,10,12,17	2,6,8,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,10,12,16,18	2,6,8,11,15,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,10,12,14	2,6,8,11	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,10,12,14,16,17,18	2,6,8,11,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,10,12,14,18	2,6,8,11,15,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,10,12,14,16,17	2,6,8,11,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,10,12,17	2,6,8,11,13,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,10,12,16,18	2,6,8,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,10,12,17,18	2,6,8,11,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,10,12,16	2,6,8,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,10,12,14,18	2,6,8,11,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,10,12,14,16,17	2,6,8,11,13,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,10,12,14	2,6,8,11,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,10,12,14,16,17,18	2,6,8,11,13,15,17,18	2^{-12}

Table 0.1901 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,17,18	2,6,8,9,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,16	2,6,8,9	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,17	2,6,8,9,15,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,16,18	2,6,8,9,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,14	2,6,8,9	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,14,16,17,18	2,6,8,9,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,14,18	2,6,8,9,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,14,16,17	2,6,8,9,15,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,17	2,6,8,9,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,16,18	2,6,8,9,13,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,17,18	2,6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,16	2,6,8,9,13,15	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,14,18	2,6,8,9,13,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,14,16,17	2,6,8,9,13,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,14	2,6,8,9,13,15	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,14,16,17,18	2,6,8,9,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,12	2,6,8,9	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,12,16,17,18	2,6,8,9,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,12,18	2,6,8,9,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,12,16,17	2,6,8,9,15,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,12,14,17,18	2,6,8,9,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,12,14,16	2,6,8,9	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,12,14,17	2,6,8,9,15,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,12,14,16,18	2,6,8,9,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,12,18	2,6,8,9,13,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,12,16,17	2,6,8,9,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,12	2,6,8,9,13,15	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,12,16,17,18	2,6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,12,14,17	2,6,8,9,13,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,12,14,16,18	2,6,8,9,13,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,12,14,17,18	2,6,8,9,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,12,14,16	2,6,8,9,13,15	2^{-23}

Table 0.1902 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,17	2,6,8,9,11,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,16,18	2,6,8,9,11,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,17,18	2,6,8,9,11,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,16	2,6,8,9,11,15	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,14,18	2,6,8,9,11,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,14,16,17	2,6,8,9,11,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,14	2,6,8,9,11,15	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,14,16,17,18	2,6,8,9,11,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,17,18	2,6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,16	2,6,8,9,11,13	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,17	2,6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,16,18	2,6,8,9,11,13,15,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,14	2,6,8,9,11,13	2^{-34}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,14,16,17,18	2,6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,14,18	2,6,8,9,11,13,15,18	2^{-34}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,14,16,17	2,6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,12,18	2,6,8,9,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,12,16,17	2,6,8,9,11,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,12	2,6,8,9,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,12,16,17,18	2,6,8,9,11,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,12,14,17	2,6,8,9,11,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,12,14,16,18	2,6,8,9,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,12,14,17,18	2,6,8,9,11,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,12,14,16	2,6,8,9,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,12	2,6,8,9,11,13	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,12,16,17,18	2,6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,12,18	2,6,8,9,11,13,15,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,12,16,17	2,6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,12,14,17,18	2,6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,12,14,16	2,6,8,9,11,13	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,12,14,17	2,6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,12,14,16,18	2,6,8,9,11,13,15,18	2^{-12}

Table 0.1903 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,10	2,6,8,9	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,10,16,17,18	2,6,8,9,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,10,18	2,6,8,9,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,10,16,17	2,6,8,9,15,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,10,14,17,18	2,6,8,9,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,10,14,16	2,6,8,9	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,10,14,17	2,6,8,9,15,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,10,14,16,18	2,6,8,9,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,10,18	2,6,8,9,13,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,10,16,17	2,6,8,9,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,10	2,6,8,9,13,15	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,10,16,17,18	2,6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,10,14,17	2,6,8,9,13,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,10,14,16,18	2,6,8,9,13,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,10,14,17,18	2,6,8,9,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,10,14,16	2,6,8,9,13,15	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,10,12,17,18	2,6,8,9,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,10,12,16	2,6,8,9	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,10,12,17	2,6,8,9,15,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,10,12,16,18	2,6,8,9,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,10,12,14	2,6,8,9	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,10,12,14,16,17,18	2,6,8,9,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,10,12,14,18	2,6,8,9,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,10,12,14,16,17	2,6,8,9,15,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,10,12,17	2,6,8,9,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,10,12,16,18	2,6,8,9,13,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,10,12,17,18	2,6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,10,12,16	2,6,8,9,13,15	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,10,12,14,18	2,6,8,9,13,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,10,12,14,16,17	2,6,8,9,13,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,10,12,14	2,6,8,9,13,15	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,10,12,14,16,17,18	2,6,8,9,13,15,17,18	$2^{-6.5}$

Table 0.1904 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,10,18	2,6,8,9,11,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,10,16,17	2,6,8,9,11,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,10	2,6,8,9,11,15	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,10,16,17,18	2,6,8,9,11,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,10,14,17	2,6,8,9,11,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,10,14,16,18	2,6,8,9,11,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,10,14,17,18	2,6,8,9,11,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,10,14,16	2,6,8,9,11,15	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,10	2,6,8,9,11,13	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,10,16,17,18	2,6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,10,18	2,6,8,9,11,13,15,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,10,16,17	2,6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,10,14,17,18	2,6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,10,14,16	2,6,8,9,11,13	2^{-1}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,10,14,17	2,6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,10,14,16,18	2,6,8,9,11,13,15,18	2^{-1}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,10,12,17	2,6,8,9,11,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,10,12,16,18	2,6,8,9,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,10,12,17,18	2,6,8,9,11,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,10,12,16	2,6,8,9,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,10,12,14,18	2,6,8,9,11,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,10,12,14,16,17	2,6,8,9,11,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,10,12,14	2,6,8,9,11,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,10,12,14,16,17,18	2,6,8,9,11,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,10,12,17,18	2,6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,10,12,16	2,6,8,9,11,13	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,10,12,17	2,6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,10,12,16,18	2,6,8,9,11,13,15,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,10,12,14	2,6,8,9,11,13	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,10,12,14,16,17,18	2,6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,10,12,14,18	2,6,8,9,11,13,15,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,10,12,14,16,17	2,6,8,9,11,13,15,17	$2^{-17.5}$

Table 0.1905 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,7	2,6	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,7,16,17,18	2,6,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,7,18	2,6,15,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,7,16,17	2,6,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,7,14,17,18	2,6,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,7,14,16	2,6	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,7,14,17	2,6,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,7,14,16,18	2,6,15,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,7,18	2,6,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,7,16,17	2,6,13,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,7	2,6,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,7,16,17,18	2,6,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,7,14,17	2,6,13,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,7,14,16,18	2,6,13,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,7,14,17,18	2,6,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,7,14,16	2,6,13,15	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,7,12,17,18	2,6,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,7,12,16	2,6	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,7,12,17	2,6,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,7,12,16,18	2,6,15,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,7,12,14	2,6	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,7,12,14,16,17,18	2,6,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,7,12,14,18	2,6,15,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,7,12,14,16,17	2,6,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,7,12,17	2,6,13,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,7,12,16,18	2,6,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,7,12,17,18	2,6,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,7,12,16	2,6,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,7,12,14,18	2,6,13,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,7,12,14,16,17	2,6,13,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,7,12,14	2,6,13,15	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,7,12,14,16,17,18	2,6,13,15,17,18	2^{-12}

Table 0.1906 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,7,18	2,6,11,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,7,16,17	2,6,11,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,7	2,6,11,15	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,7,16,17,18	2,6,11,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,7,14,17	2,6,11,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,7,14,16,18	2,6,11,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,7,14,17,18	2,6,11,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,7,14,16	2,6,11,15	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,7	2,6,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7,16,17,18	2,6,11,13,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,7,18	2,6,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7,16,17	2,6,11,13,15,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,7,14,17,18	2,6,11,13,17,18	2^{-1}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,7,14,16	2,6,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,7,14,17	2,6,11,13,15,17	2^{-1}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,7,14,16,18	2,6,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,7,12,17	2,6,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,7,12,16,18	2,6,11,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,7,12,17,18	2,6,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,7,12,16	2,6,11,15	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,7,12,14,18	2,6,11,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,7,12,14,16,17	2,6,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,7,12,14	2,6,11,15	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,7,12,14,16,17,18	2,6,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,7,12,17,18	2,6,11,13,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,7,12,16	2,6,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,7,12,17	2,6,11,13,15,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,7,12,16,18	2,6,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,7,12,14	2,6,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,7,12,14,16,17,18	2,6,11,13,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,7,12,14,18	2,6,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,7,12,14,16,17	2,6,11,13,15,17	2^{-23}

Table 0.1907 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,7,10,17,18	2,6,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,7,10,16	2,6	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,7,10,17	2,6,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,7,10,16,18	2,6,15,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,14	2,6	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,7,10,14,16,17,18	2,6,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,14,18	2,6,15,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,7,10,14,16,17	2,6,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,7,10,17	2,6,13,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,7,10,16,18	2,6,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,7,10,17,18	2,6,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,7,10,16	2,6,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,14,18	2,6,13,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,7,10,14,16,17	2,6,13,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,14	2,6,13,15	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,7,10,14,16,17,18	2,6,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,7,10,12	2,6	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,10,12,16,17,18	2,6,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,7,10,12,18	2,6,15,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,10,12,16,17	2,6,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,10,12,14,17,18	2,6,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,7,10,12,14,16	2,6	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,10,12,14,17	2,6,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,7,10,12,14,16,18	2,6,15,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,7,10,12,18	2,6,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,7,10,12,16,17	2,6,13,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,7,10,12	2,6,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,7,10,12,16,17,18	2,6,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,7,10,12,14,17	2,6,13,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,7,10,12,14,16,18	2,6,13,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,7,10,12,14,17,18	2,6,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,7,10,12,14,16	2,6,13,15	$2^{-28.5}$

Table 0.1908 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,7,10,17	2,6,11,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,7,10,16,18	2,6,11,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,7,10,17,18	2,6,11,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,7,10,16	2,6,11,15	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,7,10,14,18	2,6,11,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,7,10,14,16,17	2,6,11,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,7,10,14	2,6,11,15	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,7,10,14,16,17,18	2,6,11,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,7,10,17,18	2,6,11,13,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,7,10,16	2,6,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,7,10,17	2,6,11,13,15,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,7,10,16,18	2,6,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,7,10,14	2,6,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,7,10,14,16,17,18	2,6,11,13,17,18	2^{-34}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,7,10,14,18	2,6,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,7,10,14,16,17	2,6,11,13,15,17	2^{-34}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,7,10,12,18	2,6,11,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,7,10,12,16,17	2,6,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,7,10,12	2,6,11,15	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,7,10,12,16,17,18	2,6,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,7,10,12,14,17	2,6,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,7,10,12,14,16,18	2,6,11,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,7,10,12,14,17,18	2,6,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,7,10,12,14,16	2,6,11,15	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,10,12	2,6,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,7,10,12,16,17,18	2,6,11,13,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,10,12,18	2,6,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,7,10,12,16,17	2,6,11,13,15,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,7,10,12,14,17,18	2,6,11,13,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,7,10,12,14,16	2,6,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,7,10,12,14,17	2,6,11,13,15,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,7,10,12,14,16,18	2,6,11,13,15,18	$2^{-17.5}$

Table 0.1909 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,7,18	2,6,9,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,7,16,17	2,6,9,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,7	2,6,9,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,7,16,17,18	2,6,9,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,7,14,17	2,6,9,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,7,14,16,18	2,6,9,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,7,14,17,18	2,6,9,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,7,14,16	2,6,9,15	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,7	2,6,9,13	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,7,16,17,18	2,6,9,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,7,18	2,6,9,13,15,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,7,16,17	2,6,9,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,7,14,17,18	2,6,9,13,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,7,14,16	2,6,9,13	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,7,14,17	2,6,9,13,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,7,14,16,18	2,6,9,13,15,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,7,12,17	2,6,9,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,7,12,16,18	2,6,9,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,7,12,17,18	2,6,9,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,7,12,16	2,6,9,15	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,7,12,14,18	2,6,9,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,7,12,14,16,17	2,6,9,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,7,12,14	2,6,9,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,7,12,14,16,17,18	2,6,9,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,7,12,17,18	2,6,9,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,7,12,16	2,6,9,13	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,7,12,17	2,6,9,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,7,12,16,18	2,6,9,13,15,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,7,12,14	2,6,9,13	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,7,12,14,16,17,18	2,6,9,13,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,7,12,14,18	2,6,9,13,15,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,7,12,14,16,17	2,6,9,13,15,17	$2^{-28.5}$

Table 0.1910 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,7	2,6,9,11	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7,16,17,18	2,6,9,11,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,7,18	2,6,9,11,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7,16,17	2,6,9,11,15,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,7,14,17,18	2,6,9,11,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,7,14,16	2,6,9,11	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,7,14,17	2,6,9,11,15,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,7,14,16,18	2,6,9,11,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,7,18	2,6,9,11,13,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,7,16,17	2,6,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,7	2,6,9,11,13,15	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,7,16,17,18	2,6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,7,14,17	2,6,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,7,14,16,18	2,6,9,11,13,18	2^{-34}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,7,14,17,18	2,6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,7,14,16	2,6,9,11,13,15	2^{-34}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,7,12,17,18	2,6,9,11,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,7,12,16	2,6,9,11	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,7,12,17	2,6,9,11,15,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,7,12,16,18	2,6,9,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,7,12,14	2,6,9,11	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,7,12,14,16,17,18	2,6,9,11,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,7,12,14,18	2,6,9,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,7,12,14,16,17	2,6,9,11,15,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,7,12,17	2,6,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,7,12,16,18	2,6,9,11,13,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,7,12,17,18	2,6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,7,12,16	2,6,9,11,13,15	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,7,12,14,18	2,6,9,11,13,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,7,12,14,16,17	2,6,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,7,12,14	2,6,9,11,13,15	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,7,12,14,16,17,18	2,6,9,11,13,15,17,18	$2^{-17.5}$

Table 0.1911 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,7,10,17	2,6,9,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,7,10,16,18	2,6,9,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,7,10,17,18	2,6,9,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,7,10,16	2,6,9,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,7,10,14,18	2,6,9,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,7,10,14,16,17	2,6,9,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,7,10,14	2,6,9,15	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,7,10,14,16,17,18	2,6,9,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,7,10,17,18	2,6,9,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,7,10,16	2,6,9,13	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,7,10,17	2,6,9,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,7,10,16,18	2,6,9,13,15,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,7,10,14	2,6,9,13	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,7,10,14,16,17,18	2,6,9,13,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,7,10,14,18	2,6,9,13,15,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,7,10,14,16,17	2,6,9,13,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,7,10,12,18	2,6,9,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,7,10,12,16,17	2,6,9,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,7,10,12	2,6,9,15	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,7,10,12,16,17,18	2,6,9,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,7,10,12,14,17	2,6,9,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,7,10,12,14,16,18	2,6,9,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,7,10,12,14,17,18	2,6,9,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,7,10,12,14,16	2,6,9,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,7,10,12	2,6,9,13	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,7,10,12,16,17,18	2,6,9,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,7,10,12,18	2,6,9,13,15,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,7,10,12,16,17	2,6,9,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,7,10,12,14,17,18	2,6,9,13,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,7,10,12,14,16	2,6,9,13	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,7,10,12,14,17	2,6,9,13,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,7,10,12,14,16,18	2,6,9,13,15,18	2^{-12}

Table 0.1912 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,7,10,17,18	2,6,9,11,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,7,10,16	2,6,9,11	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,7,10,17	2,6,9,11,15,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,7,10,16,18	2,6,9,11,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,7,10,14	2,6,9,11	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,7,10,14,16,17,18	2,6,9,11,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,7,10,14,18	2,6,9,11,15,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,7,10,14,16,17	2,6,9,11,15,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,7,10,17	2,6,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,7,10,16,18	2,6,9,11,13,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,7,10,17,18	2,6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,7,10,16	2,6,9,11,13,15	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,7,10,14,18	2,6,9,11,13,18	2^{-1}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,7,10,14,16,17	2,6,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,7,10,14	2,6,9,11,13,15	2^{-1}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,7,10,14,16,17,18	2,6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,7,10,12	2,6,9,11	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,7,10,12,16,17,18	2,6,9,11,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,7,10,12,18	2,6,9,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,7,10,12,16,17	2,6,9,11,15,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,7,10,12,14,17,18	2,6,9,11,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,7,10,12,14,16	2,6,9,11	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,7,10,12,14,17	2,6,9,11,15,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,7,10,12,14,16,18	2,6,9,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,7,10,12,18	2,6,9,11,13,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,7,10,12,16,17	2,6,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,7,10,12	2,6,9,11,13,15	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,7,10,12,16,17,18	2,6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,7,10,12,14,17	2,6,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,7,10,12,14,16,18	2,6,9,11,13,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,7,10,12,14,17,18	2,6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,7,10,12,14,16	2,6,9,11,13,15	2^{-23}

Table 0.1913 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,7,17,18	2,6,8,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,7,16	2,6,8	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,7,17	2,6,8,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,7,16,18	2,6,8,15,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,7,14	2,6,8	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,7,14,16,17,18	2,6,8,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,7,14,18	2,6,8,15,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,7,14,16,17	2,6,8,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,7,17	2,6,8,13,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,7,16,18	2,6,8,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,7,17,18	2,6,8,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,7,16	2,6,8,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,7,14,18	2,6,8,13,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,7,14,16,17	2,6,8,13,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,7,14	2,6,8,13,15	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,7,14,16,17,18	2,6,8,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,7,12	2,6,8	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,7,12,16,17,18	2,6,8,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,7,12,18	2,6,8,15,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,7,12,16,17	2,6,8,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,7,12,14,17,18	2,6,8,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,7,12,14,16	2,6,8	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,7,12,14,17	2,6,8,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,7,12,14,16,18	2,6,8,15,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,7,12,18	2,6,8,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,7,12,16,17	2,6,8,13,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,7,12	2,6,8,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,7,12,16,17,18	2,6,8,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,7,12,14,17	2,6,8,13,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,7,12,14,16,18	2,6,8,13,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,7,12,14,17,18	2,6,8,13,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,7,12,14,16	2,6,8,13,15	$2^{-6.5}$

Table 0.1914 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,7,17	2,6,8,11,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,7,16,18	2,6,8,11,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,7,17,18	2,6,8,11,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,7,16	2,6,8,11,15	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,7,14,18	2,6,8,11,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,7,14,16,17	2,6,8,11,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,7,14	2,6,8,11,15	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,7,14,16,17,18	2,6,8,11,15,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,7,17,18	2,6,8,11,13,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,7,16	2,6,8,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,7,17	2,6,8,11,13,15,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,7,16,18	2,6,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,7,14	2,6,8,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,7,14,16,17,18	2,6,8,11,13,17,18	2^{-1}
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,7,14,18	2,6,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,7,14,16,17	2,6,8,11,13,15,17	2^{-1}
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,7,12,18	2,6,8,11,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,7,12,16,17	2,6,8,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,7,12	2,6,8,11,15	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,7,12,16,17,18	2,6,8,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,7,12,14,17	2,6,8,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,7,12,14,16,18	2,6,8,11,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,7,12,14,17,18	2,6,8,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,7,12,14,16	2,6,8,11,15	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,7,12	2,6,8,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,7,12,16,17,18	2,6,8,11,13,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,7,12,18	2,6,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,7,12,16,17	2,6,8,11,13,15,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,7,12,14,17,18	2,6,8,11,13,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,7,12,14,16	2,6,8,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,7,12,14,17	2,6,8,11,13,15,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,7,12,14,16,18	2,6,8,11,13,15,18	$2^{-17.5}$

Table 0.1915 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10	2,6,8	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10,16,17,18	2,6,8,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,18	2,6,8,15,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10,16,17	2,6,8,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,7,10,14,17,18	2,6,8,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,7,10,14,16	2,6,8	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,7,10,14,17	2,6,8,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,7,10,14,16,18	2,6,8,15,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,18	2,6,8,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10,16,17	2,6,8,13,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10	2,6,8,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10,16,17,18	2,6,8,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,7,10,14,17	2,6,8,13,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,7,10,14,16,18	2,6,8,13,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,7,10,14,17,18	2,6,8,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,7,10,14,16	2,6,8,13,15	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,7,10,12,17,18	2,6,8,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,7,10,12,16	2,6,8	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,7,10,12,17	2,6,8,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,7,10,12,16,18	2,6,8,15,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,7,10,12,14	2,6,8	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,7,10,12,14,16,17,18	2,6,8,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,7,10,12,14,18	2,6,8,15,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,7,10,12,14,16,17	2,6,8,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,7,10,12,17	2,6,8,13,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,7,10,12,16,18	2,6,8,13,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,7,10,12,17,18	2,6,8,13,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,7,10,12,16	2,6,8,13,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,7,10,12,14,18	2,6,8,13,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,7,10,12,14,16,17	2,6,8,13,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,7,10,12,14	2,6,8,13,15	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,7,10,12,14,16,17,18	2,6,8,13,15,17,18	2^{-23}

Table 0.1916 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7,10,18	2,6,8,11,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,7,10,16,17	2,6,8,11,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7,10	2,6,8,11,15	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,7,10,16,17,18	2,6,8,11,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,7,10,14,17	2,6,8,11,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,7,10,14,16,18	2,6,8,11,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,7,10,14,17,18	2,6,8,11,15,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,7,10,14,16	2,6,8,11,15	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,7,10	2,6,8,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,7,10,16,17,18	2,6,8,11,13,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,7,10,18	2,6,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,7,10,16,17	2,6,8,11,13,15,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,7,10,14,17,18	2,6,8,11,13,17,18	2^{-34}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,7,10,14,16	2,6,8,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,7,10,14,17	2,6,8,11,13,15,17	2^{-34}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,7,10,14,16,18	2,6,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,7,10,12,17	2,6,8,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,7,10,12,16,18	2,6,8,11,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,7,10,12,17,18	2,6,8,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,7,10,12,16	2,6,8,11,15	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,7,10,12,14,18	2,6,8,11,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,7,10,12,14,16,17	2,6,8,11,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,7,10,12,14	2,6,8,11,15	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,7,10,12,14,16,17,18	2,6,8,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,7,10,12,17,18	2,6,8,11,13,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,7,10,12,16	2,6,8,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,7,10,12,17	2,6,8,11,13,15,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,7,10,12,16,18	2,6,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,7,10,12,14	2,6,8,11,13	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,7,10,12,14,16,17,18	2,6,8,11,13,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,7,10,12,14,18	2,6,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,7,10,12,14,16,17	2,6,8,11,13,15,17	2^{-12}

Table 0.1917 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,7,17	2,6,8,9,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,7,16,18	2,6,8,9,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,7,17,18	2,6,8,9,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,7,16	2,6,8,9,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,7,14,18	2,6,8,9,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,7,14,16,17	2,6,8,9,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,7,14	2,6,8,9,15	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,7,14,16,17,18	2,6,8,9,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,7,17,18	2,6,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,7,16	2,6,8,9,13	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,7,17	2,6,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,7,16,18	2,6,8,9,13,15,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,7,14	2,6,8,9,13	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,7,14,16,17,18	2,6,8,9,13,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,7,14,18	2,6,8,9,13,15,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,7,14,16,17	2,6,8,9,13,15,17	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,12,18	2,6,8,9,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,7,12,16,17	2,6,8,9,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,12	2,6,8,9,15	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,7,12,16,17,18	2,6,8,9,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,7,12,14,17	2,6,8,9,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,12,14,16,18	2,6,8,9,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,7,12,14,17,18	2,6,8,9,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,12,14,16	2,6,8,9,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,7,12	2,6,8,9,13	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,7,12,16,17,18	2,6,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,7,12,18	2,6,8,9,13,15,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,7,12,16,17	2,6,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,7,12,14,17,18	2,6,8,9,13,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,7,12,14,16	2,6,8,9,13	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,7,12,14,17	2,6,8,9,13,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,7,12,14,16,18	2,6,8,9,13,15,18	2^{-23}

Table 0.1918 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,7,17,18	2,6,8,9,11,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,7,16	2,6,8,9,11	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,7,17	2,6,8,9,11,15,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,7,16,18	2,6,8,9,11,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,7,14	2,6,8,9,11	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,7,14,16,17,18	2,6,8,9,11,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,7,14,18	2,6,8,9,11,15,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,7,14,16,17	2,6,8,9,11,15,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,7,17	2,6,8,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,7,16,18	2,6,8,9,11,13,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,7,17,18	2,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,7,16	2,6,8,9,11,13,15	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,7,14,18	2,6,8,9,11,13,18	2^{-34}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,7,14,16,17	2,6,8,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,7,14	2,6,8,9,11,13,15	2^{-34}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,7,14,16,17,18	2,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,7,12	2,6,8,9,11	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,7,12,16,17,18	2,6,8,9,11,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,7,12,18	2,6,8,9,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,7,12,16,17	2,6,8,9,11,15,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,7,12,14,17,18	2,6,8,9,11,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,7,12,14,16	2,6,8,9,11	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,7,12,14,17	2,6,8,9,11,15,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,7,12,14,16,18	2,6,8,9,11,15,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,7,12,18	2,6,8,9,11,13,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,12,16,17	2,6,8,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,7,12	2,6,8,9,11,13,15	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,12,16,17,18	2,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,7,12,14,17	2,6,8,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,7,12,14,16,18	2,6,8,9,11,13,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,7,12,14,17,18	2,6,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,7,12,14,16	2,6,8,9,11,13,15	2^{-12}

Table 0.1919 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,7,10,18	2,6,8,9,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,7,10,16,17	2,6,8,9,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,7,10	2,6,8,9,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,7,10,16,17,18	2,6,8,9,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,7,10,14,17	2,6,8,9,17	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,7,10,14,16,18	2,6,8,9,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,7,10,14,17,18	2,6,8,9,15,17,18	2^{-23}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,7,10,14,16	2,6,8,9,15	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,7,10	2,6,8,9,13	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,7,10,16,17,18	2,6,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,7,10,18	2,6,8,9,13,15,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,7,10,16,17	2,6,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,7,10,14,17,18	2,6,8,9,13,17,18	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,7,10,14,16	2,6,8,9,13	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,7,10,14,17	2,6,8,9,13,15,17	$2^{-28.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,7,10,14,16,18	2,6,8,9,13,15,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,7,10,12,17	2,6,8,9,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,7,10,12,16,18	2,6,8,9,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,7,10,12,17,18	2,6,8,9,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,7,10,12,16	2,6,8,9,15	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,7,10,12,14,18	2,6,8,9,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,7,10,12,14,16,17	2,6,8,9,17	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,7,10,12,14	2,6,8,9,15	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,7,10,12,14,16,17,18	2,6,8,9,15,17,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,7,10,12,17,18	2,6,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,7,10,12,16	2,6,8,9,13	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,7,10,12,17	2,6,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,7,10,12,16,18	2,6,8,9,13,15,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,7,10,12,14	2,6,8,9,13	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,7,10,12,14,16,17,18	2,6,8,9,13,17,18	$2^{-6.5}$
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,7,10,12,14,18	2,6,8,9,13,15,18	2^{-12}
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,7,10,12,14,16,17	2,6,8,9,13,15,17	$2^{-6.5}$

Table 0.1920 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		P
	j values (i odd)	j values (i even)	
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,7,10	2,6,8,9,11	2 ⁻
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,7,10,16,17,18	2,6,8,9,11,17,18	2 ⁻
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,7,10,18	2,6,8,9,11,15,18	2 ⁻
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,7,10,16,17	2,6,8,9,11,15,17	2 ⁻
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,7,10,14,17,18	2,6,8,9,11,17,18	2 ⁻
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,7,10,14,16	2,6,8,9,11	2 ⁻
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,7,10,14,17	2,6,8,9,11,15,17	2 ⁻
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,7,10,14,16,18	2,6,8,9,11,15,18	2 ⁻
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7,10,18	2,6,8,9,11,13,18	2 ⁻
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,7,10,16,17	2,6,8,9,11,13,17	2 ⁻
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7,10	2,6,8,9,11,13,15	2 ⁻
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,7,10,16,17,18	2,6,8,9,11,13,15,17,18	2 ⁻
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,7,10,14,17	2,6,8,9,11,13,17	2 ⁻
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,7,10,14,16,18	2,6,8,9,11,13,18	2 ⁻
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,7,10,14,17,18	2,6,8,9,11,13,15,17,18	2 ⁻
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,7,10,14,16	2,6,8,9,11,13,15	2 ⁻
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,7,10,12,17,18	2,6,8,9,11,17,18	2 ⁻
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,7,10,12,16	2,6,8,9,11	2 ⁻
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,7,10,12,17	2,6,8,9,11,15,17	2 ⁻
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,7,10,12,16,18	2,6,8,9,11,15,18	2 ⁻
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,7,10,12,14	2,6,8,9,11	2 ⁻
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,7,10,12,14,16,17,18	2,6,8,9,11,17,18	2 ⁻
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,7,10,12,14,18	2,6,8,9,11,15,18	2 ⁻
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,7,10,12,14,16,17	2,6,8,9,11,15,17	2 ⁻
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,7,10,12,17	2,6,8,9,11,13,17	2 ⁻
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,7,10,12,16,18	2,6,8,9,11,13,18	2 ⁻
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,7,10,12,17,18	2,6,8,9,11,13,15,17,18	2 ⁻
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,7,10,12,16	2,6,8,9,11,13,15	2 ⁻
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,7,10,12,14,18	2,6,8,9,11,13,18	2 ⁻
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,7,10,12,14,16,17	2,6,8,9,11,13,17	2 ⁻
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,7,10,12,14	2,6,8,9,11,13,15	2 ⁻
$(1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,7,10,12,14,16,17,18	2,6,8,9,11,13,15,17,18	2 ⁻

Table 0.1921 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3	2,4	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,16,17,18	2,4,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,18	2,4,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,16,17	2,4,15,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,14,17,18	2,4,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,14,16	2,4	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,14,17	2,4,15,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,14,16,18	2,4,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,18	2,4,13,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,16,17	2,4,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3	2,4,13,15	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0)$	1,3,16,17,18	2,4,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,14,17	2,4,13,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,14,16,18	2,4,13,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,14,17,18	2,4,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,14,16	2,4,13,15	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,12,17,18	2,4,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,12,16	2,4	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,12,17	2,4,15,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,12,16,18	2,4,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,12,14	2,4	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,12,14,16,17,18	2,4,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,12,14,18	2,4,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,12,14,16,17	2,4,15,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,12,17	2,4,13,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,12,16,18	2,4,13,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,12,17,18	2,4,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,12,16	2,4,13,15	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,12,14,18	2,4,13,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,12,14,16,17	2,4,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,12,14	2,4,13,15	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,12,14,16,17,18	2,4,13,15,17,18	$2^{-17.5}$

Table 0.1922 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,18	2,4,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,16,17	2,4,11,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3	2,4,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,16,17,18	2,4,11,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,14,17	2,4,11,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,14,16,18	2,4,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,14,17,18	2,4,11,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,14,16	2,4,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3	2,4,11,13	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,16,17,18	2,4,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,18	2,4,11,13,15,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,16,17	2,4,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,14,17,18	2,4,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,14,16	2,4,11,13	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$	1,3,14,17	2,4,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,14,16,18	2,4,11,13,15,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,12,17	2,4,11,17	2^{-1}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,12,16,18	2,4,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,12,17,18	2,4,11,15,17,18	2^{-1}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,12,16	2,4,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,12,14,18	2,4,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,12,14,16,17	2,4,11,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,12,14	2,4,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,12,14,16,17,18	2,4,11,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,12,17,18	2,4,11,13,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1)$	1,3,12,16	2,4,11,13	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,12,17	2,4,11,13,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,12,16,18	2,4,11,13,15,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,12,14	2,4,11,13	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,12,14,16,17,18	2,4,11,13,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,12,14,18	2,4,11,13,15,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,12,14,16,17	2,4,11,13,15,17	$2^{-6.5}$

Table 0.1923 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,10,17,18	2,4,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,10,16	2,4	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,10,17	2,4,15,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,10,16,18	2,4,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,10,14	2,4	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,10,14,16,17,18	2,4,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,10,14,18	2,4,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,10,14,16,17	2,4,15,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,10,17	2,4,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1)$	1,3,10,16,18	2,4,13,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,10,17,18	2,4,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,10,16	2,4,13,15	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0)$	1,3,10,14,18	2,4,13,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,10,14,16,17	2,4,13,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,10,14	2,4,13,15	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,10,14,16,17,18	2,4,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,10,12	2,4	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,10,12,16,17,18	2,4,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,10,12,18	2,4,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,10,12,16,17	2,4,15,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,10,12,14,17,18	2,4,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,10,12,14,16	2,4	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,10,12,14,17	2,4,15,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,10,12,14,16,18	2,4,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,10,12,18	2,4,13,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,10,12,16,17	2,4,13,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,10,12	2,4,13,15	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,10,12,16,17,18	2,4,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,10,12,14,17	2,4,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,10,12,14,16,18	2,4,13,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,10,12,14,17,18	2,4,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,10,12,14,16	2,4,13,15	2^{-12}

Table 0.1924 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,10,17	2,4,11,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,10,16,18	2,4,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,10,17,18	2,4,11,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,10,16	2,4,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,10,14,18	2,4,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,10,14,16,17	2,4,11,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,10,14	2,4,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,10,14,16,17,18	2,4,11,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,10,17,18	2,4,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,10,16	2,4,11,13	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,10,17	2,4,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,10,16,18	2,4,11,13,15,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,10,14	2,4,11,13	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,10,14,16,17,18	2,4,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,10,14,18	2,4,11,13,15,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,10,14,16,17	2,4,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,10,12,18	2,4,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,10,12,16,17	2,4,11,17	2^{-34}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,10,12	2,4,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,10,12,16,17,18	2,4,11,15,17,18	2^{-34}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,10,12,14,17	2,4,11,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,10,12,14,16,18	2,4,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,10,12,14,17,18	2,4,11,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,10,12,14,16	2,4,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,10,12	2,4,11,13	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,10,12,16,17,18	2,4,11,13,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,10,12,18	2,4,11,13,15,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,10,12,16,17	2,4,11,13,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,10,12,14,17,18	2,4,11,13,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,10,12,14,16	2,4,11,13	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,10,12,14,17	2,4,11,13,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,10,12,14,16,18	2,4,11,13,15,18	2^{-23}

Table 0.1925 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,18	2,4,9,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,16,17	2,4,9,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3	2,4,9,15	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,16,17,18	2,4,9,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,14,17	2,4,9,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,14,16,18	2,4,9,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,14,17,18	2,4,9,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,14,16	2,4,9,15	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3	2,4,9,13	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0)$	1,3,16,17,18	2,4,9,13,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,18	2,4,9,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,16,17	2,4,9,13,15,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,14,17,18	2,4,9,13,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,14,16	2,4,9,13	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,14,17	2,4,9,13,15,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,14,16,18	2,4,9,13,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,12,17	2,4,9,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,12,16,18	2,4,9,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,12,17,18	2,4,9,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,12,16	2,4,9,15	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,12,14,18	2,4,9,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,12,14,16,17	2,4,9,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,12,14	2,4,9,15	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,12,14,16,17,18	2,4,9,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,12,17,18	2,4,9,13,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,12,16	2,4,9,13	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,12,17	2,4,9,13,15,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,12,16,18	2,4,9,13,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,12,14	2,4,9,13	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0)$	1,3,12,14,16,17,18	2,4,9,13,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,12,14,18	2,4,9,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,12,14,16,17	2,4,9,13,15,17	2^{-12}

Table 0.1926 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3	2,4,9,11	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,16,17,18	2,4,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,18	2,4,9,11,15,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,16,17	2,4,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,14,17,18	2,4,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,14,16	2,4,9,11	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,14,17	2,4,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,14,16,18	2,4,9,11,15,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,18	2,4,9,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,16,17	2,4,9,11,13,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3	2,4,9,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,16,17,18	2,4,9,11,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,14,17	2,4,9,11,13,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,14,16,18	2,4,9,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,14,17,18	2,4,9,11,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,14,16	2,4,9,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,12,17,18	2,4,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,12,16	2,4,9,11	2^{-34}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,12,17	2,4,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,12,16,18	2,4,9,11,15,18	2^{-34}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,12,14	2,4,9,11	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,12,14,16,17,18	2,4,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,12,14,18	2,4,9,11,15,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,12,14,16,17	2,4,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,12,17	2,4,9,11,13,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,12,16,18	2,4,9,11,13,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,12,17,18	2,4,9,11,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,12,16	2,4,9,11,13,15	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,12,14,18	2,4,9,11,13,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,12,14,16,17	2,4,9,11,13,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,12,14	2,4,9,11,13,15	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,12,14,16,17,18	2,4,9,11,13,15,17,18	2^{-23}

Table 0.1927 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,10,17	2,4,9,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,10,16,18	2,4,9,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,10,17,18	2,4,9,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,10,16	2,4,9,15	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,10,14,18	2,4,9,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,10,14,16,17	2,4,9,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0)$	1,3,10,14	2,4,9,15	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,10,14,16,17,18	2,4,9,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,10,17,18	2,4,9,13,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,10,16	2,4,9,13	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,10,17	2,4,9,13,15,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,10,16,18	2,4,9,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,10,14	2,4,9,13	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,10,14,16,17,18	2,4,9,13,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,10,14,18	2,4,9,13,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,10,14,16,17	2,4,9,13,15,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,10,12,18	2,4,9,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,10,12,16,17	2,4,9,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,10,12	2,4,9,15	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,10,12,16,17,18	2,4,9,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,10,12,14,17	2,4,9,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,10,12,14,16,18	2,4,9,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,10,12,14,17,18	2,4,9,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,10,12,14,16	2,4,9,15	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,10,12	2,4,9,13	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,10,12,16,17,18	2,4,9,13,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,10,12,18	2,4,9,13,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,10,12,16,17	2,4,9,13,15,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,10,12,14,17,18	2,4,9,13,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0)$	1,3,10,12,14,16	2,4,9,13	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,10,12,14,17	2,4,9,13,15,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,10,12,14,16,18	2,4,9,13,15,18	$2^{-17.5}$

Table 0.1928 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,10,17,18	2,4,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,10,16	2,4,9,11	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,10,17	2,4,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,10,16,18	2,4,9,11,15,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,10,14	2,4,9,11	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,10,14,16,17,18	2,4,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,10,14,18	2,4,9,11,15,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,10,14,16,17	2,4,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,10,17	2,4,9,11,13,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,10,16,18	2,4,9,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,10,17,18	2,4,9,11,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,10,16	2,4,9,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,10,14,18	2,4,9,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,10,14,16,17	2,4,9,11,13,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,10,14	2,4,9,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,10,14,16,17,18	2,4,9,11,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,10,12	2,4,9,11	2^{-1}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,10,12,16,17,18	2,4,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,10,12,18	2,4,9,11,15,18	2^{-1}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,10,12,16,17	2,4,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,10,12,14,17,18	2,4,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,10,12,14,16	2,4,9,11	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,10,12,14,17	2,4,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,10,12,14,16,18	2,4,9,11,15,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,10,12,18	2,4,9,11,13,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,10,12,16,17	2,4,9,11,13,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,10,12	2,4,9,11,13,15	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,10,12,16,17,18	2,4,9,11,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,10,12,14,17	2,4,9,11,13,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,10,12,14,16,18	2,4,9,11,13,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,10,12,14,17,18	2,4,9,11,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,10,12,14,16	2,4,9,11,13,15	$2^{-6.5}$

Table 0.1929 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,17,18	2,4,8,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,16	2,4,8	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,17	2,4,8,15,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,16,18	2,4,8,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,14	2,4,8	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,14,16,17,18	2,4,8,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,14,18	2,4,8,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,14,16,17	2,4,8,15,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,17	2,4,8,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,16,18	2,4,8,13,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1)$	1,3,17,18	2,4,8,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,16	2,4,8,13,15	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,14,18	2,4,8,13,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,14,16,17	2,4,8,13,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,14	2,4,8,13,15	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,14,16,17,18	2,4,8,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,12	2,4,8	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,12,16,17,18	2,4,8,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,12,18	2,4,8,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,12,16,17	2,4,8,15,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,12,14,17,18	2,4,8,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,12,14,16	2,4,8	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,12,14,17	2,4,8,15,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,12,14,16,18	2,4,8,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,12,18	2,4,8,13,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,12,16,17	2,4,8,13,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,12	2,4,8,13,15	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,12,16,17,18	2,4,8,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,12,14,17	2,4,8,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,12,14,16,18	2,4,8,13,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,12,14,17,18	2,4,8,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,12,14,16	2,4,8,13,15	2^{-23}

Table 0.1930 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,17	2,4,8,11,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,16,18	2,4,8,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,17,18	2,4,8,11,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,16	2,4,8,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,14,18	2,4,8,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,14,16,17	2,4,8,11,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,14	2,4,8,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,14,16,17,18	2,4,8,11,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,17,18	2,4,8,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,16	2,4,8,11,13	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,17	2,4,8,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,16,18	2,4,8,11,13,15,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,14	2,4,8,11,13	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,14,16,17,18	2,4,8,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,14,18	2,4,8,11,13,15,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,14,16,17	2,4,8,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,12,18	2,4,8,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,12,16,17	2,4,8,11,17	2^{-1}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,12	2,4,8,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,12,16,17,18	2,4,8,11,15,17,18	2^{-1}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,12,14,17	2,4,8,11,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,12,14,16,18	2,4,8,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,12,14,17,18	2,4,8,11,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,12,14,16	2,4,8,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,12	2,4,8,11,13	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,12,16,17,18	2,4,8,11,13,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,12,18	2,4,8,11,13,15,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,12,16,17	2,4,8,11,13,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,12,14,17,18	2,4,8,11,13,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,12,14,16	2,4,8,11,13	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,12,14,17	2,4,8,11,13,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,12,14,16,18	2,4,8,11,13,15,18	2^{-12}

Table 0.1931 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,10	2,4,8	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,10,16,17,18	2,4,8,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,10,18	2,4,8,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,10,16,17	2,4,8,15,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,10,14,17,18	2,4,8,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,10,14,16	2,4,8	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,10,14,17	2,4,8,15,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,10,14,16,18	2,4,8,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,10,18	2,4,8,13,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,10,16,17	2,4,8,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,10	2,4,8,13,15	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,10,16,17,18	2,4,8,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,10,14,17	2,4,8,13,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1)$	1,3,10,14,16,18	2,4,8,13,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,10,14,17,18	2,4,8,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,10,14,16	2,4,8,13,15	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,10,12,17,18	2,4,8,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,10,12,16	2,4,8	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,10,12,17	2,4,8,15,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,10,12,16,18	2,4,8,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,10,12,14	2,4,8	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,10,12,14,16,17,18	2,4,8,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,10,12,14,18	2,4,8,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,10,12,14,16,17	2,4,8,15,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,10,12,17	2,4,8,13,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,10,12,16,18	2,4,8,13,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,10,12,17,18	2,4,8,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,10,12,16	2,4,8,13,15	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,10,12,14,18	2,4,8,13,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,10,12,14,16,17	2,4,8,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,10,12,14	2,4,8,13,15	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,10,12,14,16,17,18	2,4,8,13,15,17,18	$2^{-17.5}$

Table 0.1932 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,10,18	2,4,8,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,10,16,17	2,4,8,11,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,10	2,4,8,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,10,16,17,18	2,4,8,11,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,10,14,17	2,4,8,11,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,10,14,16,18	2,4,8,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,10,14,17,18	2,4,8,11,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,10,14,16	2,4,8,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,10	2,4,8,11,13	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,10,16,17,18	2,4,8,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,10,18	2,4,8,11,13,15,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,10,16,17	2,4,8,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,10,14,17,18	2,4,8,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,10,14,16	2,4,8,11,13	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,10,14,17	2,4,8,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,10,14,16,18	2,4,8,11,13,15,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,10,12,17	2,4,8,11,17	2^{-34}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,10,12,16,18	2,4,8,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,10,12,17,18	2,4,8,11,15,17,18	2^{-34}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,10,12,16	2,4,8,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,10,12,14,18	2,4,8,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,10,12,14,16,17	2,4,8,11,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,10,12,14	2,4,8,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,10,12,14,16,17,18	2,4,8,11,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,10,12,17,18	2,4,8,11,13,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,10,12,16	2,4,8,11,13	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,10,12,17	2,4,8,11,13,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,10,12,16,18	2,4,8,11,13,15,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,10,12,14	2,4,8,11,13	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,10,12,14,16,17,18	2,4,8,11,13,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,10,12,14,18	2,4,8,11,13,15,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,10,12,14,16,17	2,4,8,11,13,15,17	$2^{-28.5}$

Table 0.1933 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,17	2,4,8,9,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,16,18	2,4,8,9,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,17,18	2,4,8,9,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,16	2,4,8,9,15	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,14,18	2,4,8,9,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,14,16,17	2,4,8,9,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,14	2,4,8,9,15	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,14,16,17,18	2,4,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,17,18	2,4,8,9,13,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,16	2,4,8,9,13	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,17	2,4,8,9,13,15,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,16,18	2,4,8,9,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,14	2,4,8,9,13	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,14,16,17,18	2,4,8,9,13,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,14,18	2,4,8,9,13,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,14,16,17	2,4,8,9,13,15,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,12,18	2,4,8,9,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,12,16,17	2,4,8,9,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,12	2,4,8,9,15	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,12,16,17,18	2,4,8,9,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,12,14,17	2,4,8,9,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,12,14,16,18	2,4,8,9,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,12,14,17,18	2,4,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,12,14,16	2,4,8,9,15	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,12	2,4,8,9,13	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,12,16,17,18	2,4,8,9,13,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,12,18	2,4,8,9,13,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,12,16,17	2,4,8,9,13,15,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,12,14,17,18	2,4,8,9,13,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,12,14,16	2,4,8,9,13	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,12,14,17	2,4,8,9,13,15,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,12,14,16,18	2,4,8,9,13,15,18	$2^{-17.5}$

Table 0.1934 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,17,18	2,4,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,16	2,4,8,9,11	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,17	2,4,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,16,18	2,4,8,9,11,15,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,14	2,4,8,9,11	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,14,16,17,18	2,4,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,14,18	2,4,8,9,11,15,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,14,16,17	2,4,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,17	2,4,8,9,11,13,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,16,18	2,4,8,9,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,17,18	2,4,8,9,11,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,16	2,4,8,9,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,14,18	2,4,8,9,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,14,16,17	2,4,8,9,11,13,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,14	2,4,8,9,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,14,16,17,18	2,4,8,9,11,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,12	2,4,8,9,11	2^{-34}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,12,16,17,18	2,4,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,12,18	2,4,8,9,11,15,18	2^{-34}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,12,16,17	2,4,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,12,14,17,18	2,4,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,12,14,16	2,4,8,9,11	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,12,14,17	2,4,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,12,14,16,18	2,4,8,9,11,15,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,12,18	2,4,8,9,11,13,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,12,16,17	2,4,8,9,11,13,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,12	2,4,8,9,11,13,15	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,12,16,17,18	2,4,8,9,11,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,12,14,17	2,4,8,9,11,13,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,12,14,16,18	2,4,8,9,11,13,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,12,14,17,18	2,4,8,9,11,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,12,14,16	2,4,8,9,11,13,15	$2^{-28.5}$

Table 0.1935 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,10,18	2,4,8,9,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,10,16,17	2,4,8,9,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,10	2,4,8,9,15	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,10,16,17,18	2,4,8,9,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,10,14,17	2,4,8,9,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,10,14,16,18	2,4,8,9,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,10,14,17,18	2,4,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,10,14,16	2,4,8,9,15	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,10	2,4,8,9,13	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,10,16,17,18	2,4,8,9,13,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,10,18	2,4,8,9,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,10,16,17	2,4,8,9,13,15,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,10,14,17,18	2,4,8,9,13,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,10,14,16	2,4,8,9,13	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,10,14,17	2,4,8,9,13,15,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,10,14,16,18	2,4,8,9,13,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,10,12,17	2,4,8,9,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,10,12,16,18	2,4,8,9,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,10,12,17,18	2,4,8,9,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,10,12,16	2,4,8,9,15	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,10,12,14,18	2,4,8,9,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,10,12,14,16,17	2,4,8,9,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,10,12,14	2,4,8,9,15	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,10,12,14,16,17,18	2,4,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,10,12,17,18	2,4,8,9,13,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,10,12,16	2,4,8,9,13	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,10,12,17	2,4,8,9,13,15,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,10,12,16,18	2,4,8,9,13,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,10,12,14	2,4,8,9,13	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,10,12,14,16,17,18	2,4,8,9,13,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,10,12,14,18	2,4,8,9,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,10,12,14,16,17	2,4,8,9,13,15,17	2^{-23}

Table 0.1936 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,10	2,4,8,9,11	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,10,16,17,18	2,4,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,10,18	2,4,8,9,11,15,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,10,16,17	2,4,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,10,14,17,18	2,4,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,10,14,16	2,4,8,9,11	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,10,14,17	2,4,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,10,14,16,18	2,4,8,9,11,15,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,10,18	2,4,8,9,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,10,16,17	2,4,8,9,11,13,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,10	2,4,8,9,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,10,16,17,18	2,4,8,9,11,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,10,14,17	2,4,8,9,11,13,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,10,14,16,18	2,4,8,9,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,10,14,17,18	2,4,8,9,11,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,10,14,16	2,4,8,9,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,10,12,17,18	2,4,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,10,12,16	2,4,8,9,11	2^{-1}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,10,12,17	2,4,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,10,12,16,18	2,4,8,9,11,15,18	2^{-1}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,10,12,14	2,4,8,9,11	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,10,12,14,16,17,18	2,4,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,10,12,14,18	2,4,8,9,11,15,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0)$	1,3,10,12,14,16,17	2,4,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,10,12,17	2,4,8,9,11,13,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,10,12,16,18	2,4,8,9,11,13,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,10,12,17,18	2,4,8,9,11,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1)$	1,3,10,12,16	2,4,8,9,11,13,15	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,10,12,14,18	2,4,8,9,11,13,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,10,12,14,16,17	2,4,8,9,11,13,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,10,12,14	2,4,8,9,11,13,15	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,10,12,14,16,17,18	2,4,8,9,11,13,15,17,18	2^{-12}

Table 0.1937 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,7,18	2,4,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,7,16,17	2,4,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,7	2,4,15	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,7,16,17,18	2,4,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,7,14,17	2,4,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,7,14,16,18	2,4,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,7,14,17,18	2,4,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,7,14,16	2,4,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,7	2,4,13	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,7,16,17,18	2,4,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,7,18	2,4,13,15,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,7,16,17	2,4,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,7,14,17,18	2,4,13,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,7,14,16	2,4,13	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,7,14,17	2,4,13,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,7,14,16,18	2,4,13,15,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,7,12,17	2,4,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,7,12,16,18	2,4,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,7,12,17,18	2,4,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,7,12,16	2,4,15	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,7,12,14,18	2,4,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,7,12,14,16,17	2,4,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,7,12,14	2,4,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,7,12,14,16,17,18	2,4,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,7,12,17,18	2,4,13,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,7,12,16	2,4,13	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,7,12,17	2,4,13,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,7,12,16,18	2,4,13,15,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,7,12,14	2,4,13	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,7,12,14,16,17,18	2,4,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,7,12,14,18	2,4,13,15,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,7,12,14,16,17	2,4,13,15,17	$2^{-17.5}$

Table 0.1938 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,7	2,4,11	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,7,16,17,18	2,4,11,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,7,18	2,4,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,7,16,17	2,4,11,15,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,7,14,17,18	2,4,11,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,7,14,16	2,4,11	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,7,14,17	2,4,11,15,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,7,14,16,18	2,4,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,7,18	2,4,11,13,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,7,16,17	2,4,11,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,7	2,4,11,13,15	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,7,16,17,18	2,4,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,7,14,17	2,4,11,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,7,14,16,18	2,4,11,13,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,7,14,17,18	2,4,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,7,14,16	2,4,11,13,15	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,7,12,17,18	2,4,11,17,18	2^{-1}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,7,12,16	2,4,11	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,7,12,17	2,4,11,15,17	2^{-1}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,7,12,16,18	2,4,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,7,12,14	2,4,11	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,7,12,14,16,17,18	2,4,11,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,7,12,14,18	2,4,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,7,12,14,16,17	2,4,11,15,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,7,12,17	2,4,11,13,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,7,12,16,18	2,4,11,13,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,7,12,17,18	2,4,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,7,12,16	2,4,11,13,15	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,7,12,14,18	2,4,11,13,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,7,12,14,16,17	2,4,11,13,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,7,12,14	2,4,11,13,15	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,7,12,14,16,17,18	2,4,11,13,15,17,18	$2^{-6.5}$

Table 0.1939 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,7,10,17	2,4,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,7,10,16,18	2,4,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,7,10,17,18	2,4,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,7,10,16	2,4,15	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,7,10,14,18	2,4,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,7,10,14,16,17	2,4,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,7,10,14	2,4,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,7,10,14,16,17,18	2,4,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,7,10,17,18	2,4,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,7,10,16	2,4,13	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,7,10,17	2,4,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,7,10,16,18	2,4,13,15,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,7,10,14	2,4,13	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,7,10,14,16,17,18	2,4,13,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,7,10,14,18	2,4,13,15,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,7,10,14,16,17	2,4,13,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,7,10,12,18	2,4,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,7,10,12,16,17	2,4,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,7,10,12	2,4,15	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,7,10,12,16,17,18	2,4,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,7,10,12,14,17	2,4,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,7,10,12,14,16,18	2,4,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,7,10,12,14,17,18	2,4,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,7,10,12,14,16	2,4,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,7,10,12	2,4,13	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,7,10,12,16,17,18	2,4,13,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,7,10,12,18	2,4,13,15,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,7,10,12,16,17	2,4,13,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,7,10,12,14,17,18	2,4,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,7,10,12,14,16	2,4,13	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,7,10,12,14,17	2,4,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,7,10,12,14,16,18	2,4,13,15,18	2^{-12}

Table 0.1940 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,7,10,17,18	2,4,11,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,7,10,16	2,4,11	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,7,10,17	2,4,11,15,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,7,10,16,18	2,4,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,7,10,14	2,4,11	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,7,10,14,16,17,18	2,4,11,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,7,10,14,18	2,4,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,7,10,14,16,17	2,4,11,15,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,7,10,17	2,4,11,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,7,10,16,18	2,4,11,13,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,7,10,17,18	2,4,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,7,10,16	2,4,11,13,15	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,7,10,14,18	2,4,11,13,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,7,10,14,16,17	2,4,11,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,7,10,14	2,4,11,13,15	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,7,10,14,16,17,18	2,4,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,7,10,12	2,4,11	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,7,10,12,16,17,18	2,4,11,17,18	2^{-34}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,7,10,12,18	2,4,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,7,10,12,16,17	2,4,11,15,17	2^{-34}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,7,10,12,14,17,18	2,4,11,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,7,10,12,14,16	2,4,11	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,7,10,12,14,17	2,4,11,15,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,7,10,12,14,16,18	2,4,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,7,10,12,18	2,4,11,13,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,7,10,12,16,17	2,4,11,13,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,7,10,12	2,4,11,13,15	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,7,10,12,16,17,18	2,4,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,7,10,12,14,17	2,4,11,13,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,7,10,12,14,16,18	2,4,11,13,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,7,10,12,14,17,18	2,4,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,7,10,12,14,16	2,4,11,13,15	2^{-23}

Table 0.1941 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,7	2,4,9	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,7,16,17,18	2,4,9,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,7,18	2,4,9,15,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,7,16,17	2,4,9,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,7,14,17,18	2,4,9,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,7,14,16	2,4,9	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,7,14,17	2,4,9,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,7,14,16,18	2,4,9,15,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,7,18	2,4,9,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,7,16,17	2,4,9,13,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,7	2,4,9,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,7,16,17,18	2,4,9,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,14,17	2,4,9,13,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,7,14,16,18	2,4,9,13,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,14,17,18	2,4,9,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,7,14,16	2,4,9,13,15	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,7,12,17,18	2,4,9,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,7,12,16	2,4,9	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,7,12,17	2,4,9,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,7,12,16,18	2,4,9,15,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,7,12,14	2,4,9	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,7,12,14,16,17,18	2,4,9,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,7,12,14,18	2,4,9,15,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,7,12,14,16,17	2,4,9,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,7,12,17	2,4,9,13,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,7,12,16,18	2,4,9,13,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,7,12,17,18	2,4,9,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,7,12,16	2,4,9,13,15	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,7,12,14,18	2,4,9,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,7,12,14,16,17	2,4,9,13,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,7,12,14	2,4,9,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,7,12,14,16,17,18	2,4,9,13,15,17,18	2^{-12}

Table 0.1942 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,7,18	2,4,9,11,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,7,16,17	2,4,9,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,7	2,4,9,11,15	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,7,16,17,18	2,4,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,7,14,17	2,4,9,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,7,14,16,18	2,4,9,11,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,7,14,17,18	2,4,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,7,14,16	2,4,9,11,15	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,7	2,4,9,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,7,16,17,18	2,4,9,11,13,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,7,18	2,4,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,7,16,17	2,4,9,11,13,15,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,7,14,17,18	2,4,9,11,13,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,7,14,16	2,4,9,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,7,14,17	2,4,9,11,13,15,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,7,14,16,18	2,4,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,7,12,17	2,4,9,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,7,12,16,18	2,4,9,11,18	2^{-34}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,7,12,17,18	2,4,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,7,12,16	2,4,9,11,15	2^{-34}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,7,12,14,18	2,4,9,11,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,7,12,14,16,17	2,4,9,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,7,12,14	2,4,9,11,15	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,7,12,14,16,17,18	2,4,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,7,12,17,18	2,4,9,11,13,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,7,12,16	2,4,9,11,13	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,7,12,17	2,4,9,11,13,15,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,7,12,16,18	2,4,9,11,13,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,7,12,14	2,4,9,11,13	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,7,12,14,16,17,18	2,4,9,11,13,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,7,12,14,18	2,4,9,11,13,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,7,12,14,16,17	2,4,9,11,13,15,17	2^{-23}

Table 0.1943 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,7,10,17,18	2,4,9,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,7,10,16	2,4,9	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,7,10,17	2,4,9,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,7,10,16,18	2,4,9,15,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,7,10,14	2,4,9	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,7,10,14,16,17,18	2,4,9,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,7,10,14,18	2,4,9,15,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,7,10,14,16,17	2,4,9,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,7,10,17	2,4,9,13,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,7,10,16,18	2,4,9,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,7,10,17,18	2,4,9,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,7,10,16	2,4,9,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,7,10,14,18	2,4,9,13,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,7,10,14,16,17	2,4,9,13,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,7,10,14	2,4,9,13,15	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,7,10,14,16,17,18	2,4,9,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,7,10,12	2,4,9	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,7,10,12,16,17,18	2,4,9,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,7,10,12,18	2,4,9,15,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,7,10,12,16,17	2,4,9,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,7,10,12,14,17,18	2,4,9,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,7,10,12,14,16	2,4,9	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,7,10,12,14,17	2,4,9,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,7,10,12,14,16,18	2,4,9,15,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,7,10,12,18	2,4,9,13,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,7,10,12,16,17	2,4,9,13,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,7,10,12	2,4,9,13,15	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,7,10,12,16,17,18	2,4,9,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,7,10,12,14,17	2,4,9,13,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,7,10,12,14,16,18	2,4,9,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,7,10,12,14,17,18	2,4,9,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,7,10,12,14,16	2,4,9,13,15	$2^{-17.5}$

Table 0.1944 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,7,10,17	2,4,9,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,7,10,16,18	2,4,9,11,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,7,10,17,18	2,4,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,7,10,16	2,4,9,11,15	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,7,10,14,18	2,4,9,11,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,7,10,14,16,17	2,4,9,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,7,10,14	2,4,9,11,15	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,7,10,14,16,17,18	2,4,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,7,10,17,18	2,4,9,11,13,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,7,10,16	2,4,9,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,7,10,17	2,4,9,11,13,15,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,7,10,16,18	2,4,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,7,10,14	2,4,9,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,7,10,14,16,17,18	2,4,9,11,13,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,7,10,14,18	2,4,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,7,10,14,16,17	2,4,9,11,13,15,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,7,10,12,18	2,4,9,11,18	2^{-1}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,7,10,12,16,17	2,4,9,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,7,10,12	2,4,9,11,15	2^{-1}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,7,10,12,16,17,18	2,4,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,7,10,12,14,17	2,4,9,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,7,10,12,14,16,18	2,4,9,11,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,7,10,12,14,17,18	2,4,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,7,10,12,14,16	2,4,9,11,15	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,7,10,12	2,4,9,11,13	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,7,10,12,16,17,18	2,4,9,11,13,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,7,10,12,18	2,4,9,11,13,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,7,10,12,16,17	2,4,9,11,13,15,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,7,10,12,14,17,18	2,4,9,11,13,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,7,10,12,14,16	2,4,9,11,13	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,7,10,12,14,17	2,4,9,11,13,15,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,7,10,12,14,16,18	2,4,9,11,13,15,18	$2^{-6.5}$

Table 0.1945 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,7,17	2,4,8,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,7,16,18	2,4,8,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,7,17,18	2,4,8,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,7,16	2,4,8,15	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,7,14,18	2,4,8,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,7,14,16,17	2,4,8,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,7,14	2,4,8,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,7,14,16,17,18	2,4,8,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,7,17,18	2,4,8,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,7,16	2,4,8,13	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,7,17	2,4,8,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,7,16,18	2,4,8,13,15,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,7,14	2,4,8,13	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,7,14,16,17,18	2,4,8,13,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,7,14,18	2,4,8,13,15,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,7,14,16,17	2,4,8,13,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,7,12,18	2,4,8,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,7,12,16,17	2,4,8,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,7,12	2,4,8,15	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,7,12,16,17,18	2,4,8,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,7,12,14,17	2,4,8,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,7,12,14,16,18	2,4,8,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,7,12,14,17,18	2,4,8,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,7,12,14,16	2,4,8,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,7,12	2,4,8,13	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,7,12,16,17,18	2,4,8,13,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,7,12,18	2,4,8,13,15,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,7,12,16,17	2,4,8,13,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,7,12,14,17,18	2,4,8,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,7,12,14,16	2,4,8,13	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,7,12,14,17	2,4,8,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,7,12,14,16,18	2,4,8,13,15,18	2^{-23}

Table 0.1946 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,7,17,18	2,4,8,11,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,7,16	2,4,8,11	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,7,17	2,4,8,11,15,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,7,16,18	2,4,8,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,7,14	2,4,8,11	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,7,14,16,17,18	2,4,8,11,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,7,14,18	2,4,8,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,7,14,16,17	2,4,8,11,15,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,7,17	2,4,8,11,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,7,16,18	2,4,8,11,13,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,7,17,18	2,4,8,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,7,16	2,4,8,11,13,15	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,7,14,18	2,4,8,11,13,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,7,14,16,17	2,4,8,11,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,7,14	2,4,8,11,13,15	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,7,14,16,17,18	2,4,8,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,7,12	2,4,8,11	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,7,12,16,17,18	2,4,8,11,17,18	2^{-1}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,7,12,18	2,4,8,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,7,12,16,17	2,4,8,11,15,17	2^{-1}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,7,12,14,17,18	2,4,8,11,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,7,12,14,16	2,4,8,11	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,7,12,14,17	2,4,8,11,15,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,7,12,14,16,18	2,4,8,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,7,12,18	2,4,8,11,13,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,7,12,16,17	2,4,8,11,13,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,7,12	2,4,8,11,13,15	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,7,12,16,17,18	2,4,8,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,7,12,14,17	2,4,8,11,13,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,7,12,14,16,18	2,4,8,11,13,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,7,12,14,17,18	2,4,8,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,7,12,14,16	2,4,8,11,13,15	2^{-12}

Table 0.1947 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,7,10,18	2,4,8,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,7,10,16,17	2,4,8,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,7,10	2,4,8,15	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,7,10,16,17,18	2,4,8,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,7,10,14,17	2,4,8,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,7,10,14,16,18	2,4,8,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,7,10,14,17,18	2,4,8,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,7,10,14,16	2,4,8,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,7,10	2,4,8,13	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,7,10,16,17,18	2,4,8,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,7,10,18	2,4,8,13,15,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,7,10,16,17	2,4,8,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,7,10,14,17,18	2,4,8,13,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,10,14,16	2,4,8,13	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,7,10,14,17	2,4,8,13,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,10,14,16,18	2,4,8,13,15,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,7,10,12,17	2,4,8,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,7,10,12,16,18	2,4,8,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,7,10,12,17,18	2,4,8,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,7,10,12,16	2,4,8,15	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,7,10,12,14,18	2,4,8,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,7,10,12,14,16,17	2,4,8,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,7,10,12,14	2,4,8,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,7,10,12,14,16,17,18	2,4,8,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,7,10,12,17,18	2,4,8,13,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,7,10,12,16	2,4,8,13	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,7,10,12,17	2,4,8,13,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,7,10,12,16,18	2,4,8,13,15,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,7,10,12,14	2,4,8,13	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,7,10,12,14,16,17,18	2,4,8,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,7,10,12,14,18	2,4,8,13,15,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,7,10,12,14,16,17	2,4,8,13,15,17	$2^{-17.5}$

Table 0.1948 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,7,10	2,4,8,11	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,7,10,16,17,18	2,4,8,11,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,7,10,18	2,4,8,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,7,10,16,17	2,4,8,11,15,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,7,10,14,17,18	2,4,8,11,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,7,10,14,16	2,4,8,11	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,7,10,14,17	2,4,8,11,15,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,7,10,14,16,18	2,4,8,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,7,10,18	2,4,8,11,13,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,7,10,16,17	2,4,8,11,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,7,10	2,4,8,11,13,15	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,7,10,16,17,18	2,4,8,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,7,10,14,17	2,4,8,11,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1)$	1,3,7,10,14,16,18	2,4,8,11,13,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,7,10,14,17,18	2,4,8,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,7,10,14,16	2,4,8,11,13,15	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,7,10,12,17,18	2,4,8,11,17,18	2^{-34}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,7,10,12,16	2,4,8,11	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,7,10,12,17	2,4,8,11,15,17	2^{-34}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,7,10,12,16,18	2,4,8,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,7,10,12,14	2,4,8,11	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,7,10,12,14,16,17,18	2,4,8,11,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,7,10,12,14,18	2,4,8,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,7,10,12,14,16,17	2,4,8,11,15,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,7,10,12,17	2,4,8,11,13,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,7,10,12,16,18	2,4,8,11,13,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,7,10,12,17,18	2,4,8,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,7,10,12,16	2,4,8,11,13,15	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,7,10,12,14,18	2,4,8,11,13,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,7,10,12,14,16,17	2,4,8,11,13,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,7,10,12,14	2,4,8,11,13,15	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,7,10,12,14,16,17,18	2,4,8,11,13,15,17,18	$2^{-28.5}$

Table 0.1949 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,7,17,18	2,4,8,9,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,7,16	2,4,8,9	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,7,17	2,4,8,9,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,7,16,18	2,4,8,9,15,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,7,14	2,4,8,9	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,7,14,16,17,18	2,4,8,9,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,7,14,18	2,4,8,9,15,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,7,14,16,17	2,4,8,9,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,7,17	2,4,8,9,13,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,7,16,18	2,4,8,9,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,7,17,18	2,4,8,9,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,7,16	2,4,8,9,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,7,14,18	2,4,8,9,13,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0)$	1,3,7,14,16,17	2,4,8,9,13,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,7,14	2,4,8,9,13,15	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,7,14,16,17,18	2,4,8,9,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,7,12	2,4,8,9	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,7,12,16,17,18	2,4,8,9,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,7,12,18	2,4,8,9,15,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,7,12,16,17	2,4,8,9,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,7,12,14,17,18	2,4,8,9,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,7,12,14,16	2,4,8,9	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,7,12,14,17	2,4,8,9,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,7,12,14,16,18	2,4,8,9,15,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,7,12,18	2,4,8,9,13,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,7,12,16,17	2,4,8,9,13,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,7,12	2,4,8,9,13,15	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,7,12,16,17,18	2,4,8,9,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,7,12,14,17	2,4,8,9,13,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,7,12,14,16,18	2,4,8,9,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,7,12,14,17,18	2,4,8,9,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,7,12,14,16	2,4,8,9,13,15	$2^{-17.5}$

Table 0.1950 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,7,17	2,4,8,9,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,7,16,18	2,4,8,9,11,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,7,17,18	2,4,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,7,16	2,4,8,9,11,15	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,7,14,18	2,4,8,9,11,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,7,14,16,17	2,4,8,9,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,7,14	2,4,8,9,11,15	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,7,14,16,17,18	2,4,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,7,17,18	2,4,8,9,11,13,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,7,16	2,4,8,9,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,7,17	2,4,8,9,11,13,15,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,7,16,18	2,4,8,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,7,14	2,4,8,9,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,7,14,16,17,18	2,4,8,9,11,13,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,7,14,18	2,4,8,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,7,14,16,17	2,4,8,9,11,13,15,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,7,12,18	2,4,8,9,11,18	2^{-34}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,7,12,16,17	2,4,8,9,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,7,12	2,4,8,9,11,15	2^{-34}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,7,12,16,17,18	2,4,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,7,12,14,17	2,4,8,9,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,7,12,14,16,18	2,4,8,9,11,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,7,12,14,17,18	2,4,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,7,12,14,16	2,4,8,9,11,15	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,7,12	2,4,8,9,11,13	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,7,12,16,17,18	2,4,8,9,11,13,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,7,12,18	2,4,8,9,11,13,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,7,12,16,17	2,4,8,9,11,13,15,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,7,12,14,17,18	2,4,8,9,11,13,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,7,12,14,16	2,4,8,9,11,13	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,7,12,14,17	2,4,8,9,11,13,15,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,7,12,14,16,18	2,4,8,9,11,13,15,18	$2^{-28.5}$

Table 0.1951 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,7,10	2,4,8,9	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,7,10,16,17,18	2,4,8,9,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,7,10,18	2,4,8,9,15,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,7,10,16,17	2,4,8,9,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,7,10,14,17,18	2,4,8,9,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,7,10,14,16	2,4,8,9	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,7,10,14,17	2,4,8,9,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1)$	1,3,7,10,14,16,18	2,4,8,9,15,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,7,10,18	2,4,8,9,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,7,10,16,17	2,4,8,9,13,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,7,10	2,4,8,9,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,7,10,16,17,18	2,4,8,9,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,7,10,14,17	2,4,8,9,13,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,7,10,14,16,18	2,4,8,9,13,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,7,10,14,17,18	2,4,8,9,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,7,10,14,16	2,4,8,9,13,15	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,7,10,12,17,18	2,4,8,9,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,7,10,12,16	2,4,8,9	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,7,10,12,17	2,4,8,9,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,7,10,12,16,18	2,4,8,9,15,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,7,10,12,14	2,4,8,9	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,7,10,12,14,16,17,18	2,4,8,9,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,7,10,12,14,18	2,4,8,9,15,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,7,10,12,14,16,17	2,4,8,9,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,7,10,12,17	2,4,8,9,13,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,7,10,12,16,18	2,4,8,9,13,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,7,10,12,17,18	2,4,8,9,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,7,10,12,16	2,4,8,9,13,15	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,7,10,12,14,18	2,4,8,9,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,7,10,12,14,16,17	2,4,8,9,13,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,7,10,12,14	2,4,8,9,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,7,10,12,14,16,17,18	2,4,8,9,13,15,17,18	2^{-23}

Table 0.1952 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,7,10,18	2,4,8,9,11,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,7,10,16,17	2,4,8,9,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,7,10	2,4,8,9,11,15	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,7,10,16,17,18	2,4,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,7,10,14,17	2,4,8,9,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,7,10,14,16,18	2,4,8,9,11,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,7,10,14,17,18	2,4,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,7,10,14,16	2,4,8,9,11,15	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,7,10	2,4,8,9,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,7,10,16,17,18	2,4,8,9,11,13,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,7,10,18	2,4,8,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,7,10,16,17	2,4,8,9,11,13,15,17	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,7,10,14,17,18	2,4,8,9,11,13,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,7,10,14,16	2,4,8,9,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,7,10,14,17	2,4,8,9,11,13,15,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,7,10,14,16,18	2,4,8,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,7,10,12,17	2,4,8,9,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,7,10,12,16,18	2,4,8,9,11,18	2^{-1}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,7,10,12,17,18	2,4,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,7,10,12,16	2,4,8,9,11,15	2^{-1}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,7,10,12,14,18	2,4,8,9,11,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,7,10,12,14,16,17	2,4,8,9,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,7,10,12,14	2,4,8,9,11,15	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,7,10,12,14,16,17,18	2,4,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,7,10,12,17,18	2,4,8,9,11,13,17,18	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,7,10,12,16	2,4,8,9,11,13	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,7,10,12,17	2,4,8,9,11,13,15,17	2^{-23}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,7,10,12,16,18	2,4,8,9,11,13,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,7,10,12,14	2,4,8,9,11,13	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,7,10,12,14,16,17,18	2,4,8,9,11,13,17,18	2^{-12}
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,7,10,12,14,18	2,4,8,9,11,13,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,7,10,12,14,16,17	2,4,8,9,11,13,15,17	2^{-12}

Table 0.1953 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,17,18	2,4,6,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,16	2,4,6	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,17	2,4,6,15,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,16,18	2,4,6,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,14	2,4,6	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,14,16,17,18	2,4,6,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,14,18	2,4,6,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,14,16,17	2,4,6,15,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,17	2,4,6,13,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,16,18	2,4,6,13,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1)$	1,3,17,18	2,4,6,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,16	2,4,6,13,15	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,14,18	2,4,6,13,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,14,16,17	2,4,6,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,14	2,4,6,13,15	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,14,16,17,18	2,4,6,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,12	2,4,6	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,12,16,17,18	2,4,6,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,12,18	2,4,6,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,12,16,17	2,4,6,15,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,12,14,17,18	2,4,6,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,12,14,16	2,4,6	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,12,14,17	2,4,6,15,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,12,14,16,18	2,4,6,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,12,18	2,4,6,13,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,12,16,17	2,4,6,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,12	2,4,6,13,15	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,12,16,17,18	2,4,6,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,12,14,17	2,4,6,13,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,12,14,16,18	2,4,6,13,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,12,14,17,18	2,4,6,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,12,14,16	2,4,6,13,15	2^{-23}

Table 0.1954 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,17	2,4,6,11,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,16,18	2,4,6,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,17,18	2,4,6,11,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,16	2,4,6,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,14,18	2,4,6,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,14,16,17	2,4,6,11,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,14	2,4,6,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,14,16,17,18	2,4,6,11,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,17,18	2,4,6,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,16	2,4,6,11,13	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,17	2,4,6,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,16,18	2,4,6,11,13,15,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,14	2,4,6,11,13	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,14,16,17,18	2,4,6,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,14,18	2,4,6,11,13,15,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,14,16,17	2,4,6,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,12,18	2,4,6,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,12,16,17	2,4,6,11,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,12	2,4,6,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,12,16,17,18	2,4,6,11,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,12,14,17	2,4,6,11,17	2^{-1}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,12,14,16,18	2,4,6,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,12,14,17,18	2,4,6,11,15,17,18	2^{-1}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,12,14,16	2,4,6,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,12	2,4,6,11,13	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,12,16,17,18	2,4,6,11,13,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,12,18	2,4,6,11,13,15,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,12,16,17	2,4,6,11,13,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,12,14,17,18	2,4,6,11,13,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,12,14,16	2,4,6,11,13	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,12,14,17	2,4,6,11,13,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,12,14,16,18	2,4,6,11,13,15,18	2^{-23}

Table 0.1955 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,10	2,4,6	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,10,16,17,18	2,4,6,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,10,18	2,4,6,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,10,16,17	2,4,6,15,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,10,14,17,18	2,4,6,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,10,14,16	2,4,6	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,10,14,17	2,4,6,15,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,10,14,16,18	2,4,6,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,10,18	2,4,6,13,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,10,16,17	2,4,6,13,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,10	2,4,6,13,15	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,10,16,17,18	2,4,6,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,10,14,17	2,4,6,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,10,14,16,18	2,4,6,13,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,10,14,17,18	2,4,6,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,10,14,16	2,4,6,13,15	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,10,12,17,18	2,4,6,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,10,12,16	2,4,6	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,10,12,17	2,4,6,15,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,10,12,16,18	2,4,6,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,10,12,14	2,4,6	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,10,12,14,16,17,18	2,4,6,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,10,12,14,18	2,4,6,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,10,12,14,16,17	2,4,6,15,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,10,12,17	2,4,6,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,10,12,16,18	2,4,6,13,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,10,12,17,18	2,4,6,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,10,12,16	2,4,6,13,15	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,10,12,14,18	2,4,6,13,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,10,12,14,16,17	2,4,6,13,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,10,12,14	2,4,6,13,15	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,10,12,14,16,17,18	2,4,6,13,15,17,18	$2^{-28.5}$

Table 0.1956 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,10,18	2,4,6,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,10,16,17	2,4,6,11,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,10	2,4,6,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,10,16,17,18	2,4,6,11,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,10,14,17	2,4,6,11,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,10,14,16,18	2,4,6,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,10,14,17,18	2,4,6,11,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,10,14,16	2,4,6,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,10	2,4,6,11,13	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,10,16,17,18	2,4,6,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,10,18	2,4,6,11,13,15,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,10,16,17	2,4,6,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,10,14,17,18	2,4,6,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,10,14,16	2,4,6,11,13	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,10,14,17	2,4,6,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,10,14,16,18	2,4,6,11,13,15,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,10,12,17	2,4,6,11,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,10,12,16,18	2,4,6,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,10,12,17,18	2,4,6,11,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,10,12,16	2,4,6,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,10,12,14,18	2,4,6,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,10,12,14,16,17	2,4,6,11,17	2^{-34}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,10,12,14	2,4,6,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,10,12,14,16,17,18	2,4,6,11,15,17,18	2^{-34}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,10,12,17,18	2,4,6,11,13,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,10,12,16	2,4,6,11,13	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,10,12,17	2,4,6,11,13,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,10,12,16,18	2,4,6,11,13,15,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,10,12,14	2,4,6,11,13	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,10,12,14,16,17,18	2,4,6,11,13,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,10,12,14,18	2,4,6,11,13,15,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,10,12,14,16,17	2,4,6,11,13,15,17	$2^{-28.5}$

Table 0.1957 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,17	2,4,6,9,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,16,18	2,4,6,9,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,17,18	2,4,6,9,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,16	2,4,6,9,15	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,14,18	2,4,6,9,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,14,16,17	2,4,6,9,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,14	2,4,6,9,15	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,14,16,17,18	2,4,6,9,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,17,18	2,4,6,9,13,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,16	2,4,6,9,13	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,17	2,4,6,9,13,15,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,16,18	2,4,6,9,13,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,14	2,4,6,9,13	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,14,16,17,18	2,4,6,9,13,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,14,18	2,4,6,9,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,14,16,17	2,4,6,9,13,15,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,12,18	2,4,6,9,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,12,16,17	2,4,6,9,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,12	2,4,6,9,15	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,12,16,17,18	2,4,6,9,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,12,14,17	2,4,6,9,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,12,14,16,18	2,4,6,9,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,12,14,17,18	2,4,6,9,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,12,14,16	2,4,6,9,15	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,12	2,4,6,9,13	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,12,16,17,18	2,4,6,9,13,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,12,18	2,4,6,9,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,12,16,17	2,4,6,9,13,15,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,12,14,17,18	2,4,6,9,13,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,12,14,16	2,4,6,9,13	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,12,14,17	2,4,6,9,13,15,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,12,14,16,18	2,4,6,9,13,15,18	$2^{-28.5}$

Table 0.1958 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,17,18	2,4,6,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,16	2,4,6,9,11	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,17	2,4,6,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,16,18	2,4,6,9,11,15,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,14	2,4,6,9,11	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,14,16,17,18	2,4,6,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,14,18	2,4,6,9,11,15,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,14,16,17	2,4,6,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,17	2,4,6,9,11,13,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,16,18	2,4,6,9,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,17,18	2,4,6,9,11,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,16	2,4,6,9,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,14,18	2,4,6,9,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,14,16,17	2,4,6,9,11,13,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,14	2,4,6,9,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,14,16,17,18	2,4,6,9,11,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,12	2,4,6,9,11	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,12,16,17,18	2,4,6,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,12,18	2,4,6,9,11,15,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,12,16,17	2,4,6,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,12,14,17,18	2,4,6,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,12,14,16	2,4,6,9,11	2^{-34}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,12,14,17	2,4,6,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,12,14,16,18	2,4,6,9,11,15,18	2^{-34}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,12,18	2,4,6,9,11,13,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,12,16,17	2,4,6,9,11,13,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,12	2,4,6,9,11,13,15	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,12,16,17,18	2,4,6,9,11,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,12,14,17	2,4,6,9,11,13,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,12,14,16,18	2,4,6,9,11,13,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,12,14,17,18	2,4,6,9,11,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,12,14,16	2,4,6,9,11,13,15	$2^{-28.5}$

Table 0.1959 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,10,18	2,4,6,9,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,10,16,17	2,4,6,9,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,10	2,4,6,9,15	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,10,16,17,18	2,4,6,9,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,10,14,17	2,4,6,9,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,10,14,16,18	2,4,6,9,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,10,14,17,18	2,4,6,9,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,10,14,16	2,4,6,9,15	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,10	2,4,6,9,13	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,10,16,17,18	2,4,6,9,13,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,10,18	2,4,6,9,13,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,10,16,17	2,4,6,9,13,15,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,10,14,17,18	2,4,6,9,13,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,10,14,16	2,4,6,9,13	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,10,14,17	2,4,6,9,13,15,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,10,14,16,18	2,4,6,9,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,10,12,17	2,4,6,9,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,10,12,16,18	2,4,6,9,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,10,12,17,18	2,4,6,9,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,10,12,16	2,4,6,9,15	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,10,12,14,18	2,4,6,9,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,10,12,14,16,17	2,4,6,9,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,10,12,14	2,4,6,9,15	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,10,12,14,16,17,18	2,4,6,9,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,10,12,17,18	2,4,6,9,13,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,10,12,16	2,4,6,9,13	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,10,12,17	2,4,6,9,13,15,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,10,12,16,18	2,4,6,9,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,10,12,14	2,4,6,9,13	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,10,12,14,16,17,18	2,4,6,9,13,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,10,12,14,18	2,4,6,9,13,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,10,12,14,16,17	2,4,6,9,13,15,17	2^{-23}

Table 0.1960 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,10	2,4,6,9,11	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,10,16,17,18	2,4,6,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,10,18	2,4,6,9,11,15,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,10,16,17	2,4,6,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,10,14,17,18	2,4,6,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,10,14,16	2,4,6,9,11	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,10,14,17	2,4,6,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,10,14,16,18	2,4,6,9,11,15,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,10,18	2,4,6,9,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,10,16,17	2,4,6,9,11,13,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,10	2,4,6,9,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,10,16,17,18	2,4,6,9,11,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,10,14,17	2,4,6,9,11,13,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,10,14,16,18	2,4,6,9,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,10,14,17,18	2,4,6,9,11,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,10,14,16	2,4,6,9,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,10,12,17,18	2,4,6,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,10,12,16	2,4,6,9,11	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,10,12,17	2,4,6,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,10,12,16,18	2,4,6,9,11,15,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0)$	1,3,10,12,14	2,4,6,9,11	2^{-1}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,10,12,14,16,17,18	2,4,6,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,10,12,14,18	2,4,6,9,11,15,18	2^{-1}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,10,12,14,16,17	2,4,6,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,10,12,17	2,4,6,9,11,13,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,10,12,16,18	2,4,6,9,11,13,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,10,12,17,18	2,4,6,9,11,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,10,12,16	2,4,6,9,11,13,15	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,10,12,14,18	2,4,6,9,11,13,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,10,12,14,16,17	2,4,6,9,11,13,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,10,12,14	2,4,6,9,11,13,15	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,10,12,14,16,17,18	2,4,6,9,11,13,15,17,18	2^{-23}

Table 0.1961 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3	2,4,6,8	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,16,17,18	2,4,6,8,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,18	2,4,6,8,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,16,17	2,4,6,8,15,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,14,17,18	2,4,6,8,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,14,16	2,4,6,8	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,14,17	2,4,6,8,15,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,14,16,18	2,4,6,8,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,18	2,4,6,8,13,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,16,17	2,4,6,8,13,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3	2,4,6,8,13,15	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,16,17,18	2,4,6,8,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,14,17	2,4,6,8,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,14,16,18	2,4,6,8,13,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,14,17,18	2,4,6,8,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,14,16	2,4,6,8,13,15	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,12,17,18	2,4,6,8,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,12,16	2,4,6,8	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,12,17	2,4,6,8,15,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,12,16,18	2,4,6,8,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,12,14	2,4,6,8	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,12,14,16,17,18	2,4,6,8,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,12,14,18	2,4,6,8,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0)$	1,3,12,14,16,17	2,4,6,8,15,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,12,17	2,4,6,8,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,12,16,18	2,4,6,8,13,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,12,17,18	2,4,6,8,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,12,16	2,4,6,8,13,15	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,12,14,18	2,4,6,8,13,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,12,14,16,17	2,4,6,8,13,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,12,14	2,4,6,8,13,15	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,12,14,16,17,18	2,4,6,8,13,15,17,18	$2^{-6.5}$

Table 0.1962 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,18	2,4,6,8,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,16,17	2,4,6,8,11,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3	2,4,6,8,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,16,17,18	2,4,6,8,11,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,14,17	2,4,6,8,11,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,14,16,18	2,4,6,8,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,14,17,18	2,4,6,8,11,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,14,16	2,4,6,8,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3	2,4,6,8,11,13	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,16,17,18	2,4,6,8,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,18	2,4,6,8,11,13,15,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,16,17	2,4,6,8,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,14,17,18	2,4,6,8,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,14,16	2,4,6,8,11,13	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,14,17	2,4,6,8,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,14,16,18	2,4,6,8,11,13,15,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,12,17	2,4,6,8,11,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,12,16,18	2,4,6,8,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,12,17,18	2,4,6,8,11,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,12,16	2,4,6,8,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,12,14,18	2,4,6,8,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,12,14,16,17	2,4,6,8,11,17	2^{-1}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,12,14	2,4,6,8,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,12,14,16,17,18	2,4,6,8,11,15,17,18	2^{-1}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,12,17,18	2,4,6,8,11,13,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,12,16	2,4,6,8,11,13	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,12,17	2,4,6,8,11,13,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,12,16,18	2,4,6,8,11,13,15,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,12,14	2,4,6,8,11,13	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,12,14,16,17,18	2,4,6,8,11,13,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,12,14,18	2,4,6,8,11,13,15,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,12,14,16,17	2,4,6,8,11,13,15,17	$2^{-6.5}$

Table 0.1963 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,10,17,18	2,4,6,8,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,10,16	2,4,6,8	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,10,17	2,4,6,8,15,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,10,16,18	2,4,6,8,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,10,14	2,4,6,8	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,10,14,16,17,18	2,4,6,8,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,10,14,18	2,4,6,8,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,10,14,16,17	2,4,6,8,15,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,10,17	2,4,6,8,13,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,10,16,18	2,4,6,8,13,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,10,17,18	2,4,6,8,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,10,16	2,4,6,8,13,15	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,10,14,18	2,4,6,8,13,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,10,14,16,17	2,4,6,8,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,10,14	2,4,6,8,13,15	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,10,14,16,17,18	2,4,6,8,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,10,12	2,4,6,8	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,10,12,16,17,18	2,4,6,8,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,10,12,18	2,4,6,8,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,10,12,16,17	2,4,6,8,15,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,10,12,14,17,18	2,4,6,8,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,10,12,14,16	2,4,6,8	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,10,12,14,17	2,4,6,8,15,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,10,12,14,16,18	2,4,6,8,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,10,12,18	2,4,6,8,13,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,10,12,16,17	2,4,6,8,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,10,12	2,4,6,8,13,15	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,10,12,16,17,18	2,4,6,8,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,10,12,14,17	2,4,6,8,13,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1)$	1,3,10,12,14,16,18	2,4,6,8,13,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,10,12,14,17,18	2,4,6,8,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,10,12,14,16	2,4,6,8,13,15	2^{-12}

Table 0.1964 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,10,17	2,4,6,8,11,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,10,16,18	2,4,6,8,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,10,17,18	2,4,6,8,11,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,10,16	2,4,6,8,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,10,14,18	2,4,6,8,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,10,14,16,17	2,4,6,8,11,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,10,14	2,4,6,8,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,10,14,16,17,18	2,4,6,8,11,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,10,17,18	2,4,6,8,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,10,16	2,4,6,8,11,13	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,10,17	2,4,6,8,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,10,16,18	2,4,6,8,11,13,15,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,10,14	2,4,6,8,11,13	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,10,14,16,17,18	2,4,6,8,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,10,14,18	2,4,6,8,11,13,15,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,10,14,16,17	2,4,6,8,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,10,12,18	2,4,6,8,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,10,12,16,17	2,4,6,8,11,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,10,12	2,4,6,8,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,10,12,16,17,18	2,4,6,8,11,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,10,12,14,17	2,4,6,8,11,17	2^{-34}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,10,12,14,16,18	2,4,6,8,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,10,12,14,17,18	2,4,6,8,11,15,17,18	2^{-34}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,10,12,14,16	2,4,6,8,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,10,12	2,4,6,8,11,13	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,10,12,16,17,18	2,4,6,8,11,13,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,10,12,18	2,4,6,8,11,13,15,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,10,12,16,17	2,4,6,8,11,13,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,10,12,14,17,18	2,4,6,8,11,13,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,10,12,14,16	2,4,6,8,11,13	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,10,12,14,17	2,4,6,8,11,13,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,10,12,14,16,18	2,4,6,8,11,13,15,18	2^{-12}

Table 0.1965 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,18	2,4,6,8,9,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,16,17	2,4,6,8,9,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3	2,4,6,8,9,15	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,16,17,18	2,4,6,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,14,17	2,4,6,8,9,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,14,16,18	2,4,6,8,9,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,14,17,18	2,4,6,8,9,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,14,16	2,4,6,8,9,15	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3	2,4,6,8,9,13	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,16,17,18	2,4,6,8,9,13,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,18	2,4,6,8,9,13,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,16,17	2,4,6,8,9,13,15,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,14,17,18	2,4,6,8,9,13,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,14,16	2,4,6,8,9,13	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,14,17	2,4,6,8,9,13,15,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,14,16,18	2,4,6,8,9,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,12,17	2,4,6,8,9,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,12,16,18	2,4,6,8,9,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,12,17,18	2,4,6,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,12,16	2,4,6,8,9,15	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,12,14,18	2,4,6,8,9,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,12,14,16,17	2,4,6,8,9,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,12,14	2,4,6,8,9,15	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,12,14,16,17,18	2,4,6,8,9,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,12,17,18	2,4,6,8,9,13,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,12,16	2,4,6,8,9,13	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,12,17	2,4,6,8,9,13,15,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,12,16,18	2,4,6,8,9,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,12,14	2,4,6,8,9,13	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,12,14,16,17,18	2,4,6,8,9,13,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,12,14,18	2,4,6,8,9,13,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,12,14,16,17	2,4,6,8,9,13,15,17	2^{-12}

Table 0.1966 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3	2,4,6,8,9,11	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,16,17,18	2,4,6,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,18	2,4,6,8,9,11,15,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,16,17	2,4,6,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,14,17,18	2,4,6,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,14,16	2,4,6,8,9,11	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,14,17	2,4,6,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,14,16,18	2,4,6,8,9,11,15,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,18	2,4,6,8,9,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,16,17	2,4,6,8,9,11,13,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3	2,4,6,8,9,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,16,17,18	2,4,6,8,9,11,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,14,17	2,4,6,8,9,11,13,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,14,16,18	2,4,6,8,9,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,14,17,18	2,4,6,8,9,11,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,14,16	2,4,6,8,9,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,12,17,18	2,4,6,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,12,16	2,4,6,8,9,11	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,12,17	2,4,6,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,12,16,18	2,4,6,8,9,11,15,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,12,14	2,4,6,8,9,11	2^{-34}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,12,14,16,17,18	2,4,6,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,12,14,18	2,4,6,8,9,11,15,18	2^{-34}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,12,14,16,17	2,4,6,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,12,17	2,4,6,8,9,11,13,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,12,16,18	2,4,6,8,9,11,13,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,12,17,18	2,4,6,8,9,11,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,12,16	2,4,6,8,9,11,13,15	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,12,14,18	2,4,6,8,9,11,13,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,12,14,16,17	2,4,6,8,9,11,13,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,12,14	2,4,6,8,9,11,13,15	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,12,14,16,17,18	2,4,6,8,9,11,13,15,17,18	2^{-12}

Table 0.1967 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,10,17	2,4,6,8,9,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,10,16,18	2,4,6,8,9,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,10,17,18	2,4,6,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,10,16	2,4,6,8,9,15	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,10,14,18	2,4,6,8,9,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,10,14,16,17	2,4,6,8,9,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,10,14	2,4,6,8,9,15	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,10,14,16,17,18	2,4,6,8,9,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,10,17,18	2,4,6,8,9,13,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,10,16	2,4,6,8,9,13	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,10,17	2,4,6,8,9,13,15,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,10,16,18	2,4,6,8,9,13,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,10,14	2,4,6,8,9,13	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,10,14,16,17,18	2,4,6,8,9,13,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,10,14,18	2,4,6,8,9,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,10,14,16,17	2,4,6,8,9,13,15,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,10,12,18	2,4,6,8,9,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,10,12,16,17	2,4,6,8,9,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,10,12	2,4,6,8,9,15	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,10,12,16,17,18	2,4,6,8,9,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,10,12,14,17	2,4,6,8,9,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,10,12,14,16,18	2,4,6,8,9,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,10,12,14,17,18	2,4,6,8,9,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,10,12,14,16	2,4,6,8,9,15	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,10,12	2,4,6,8,9,13	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,10,12,16,17,18	2,4,6,8,9,13,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,10,12,18	2,4,6,8,9,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,10,12,16,17	2,4,6,8,9,13,15,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,10,12,14,17,18	2,4,6,8,9,13,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,10,12,14,16	2,4,6,8,9,13	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,10,12,14,17	2,4,6,8,9,13,15,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,10,12,14,16,18	2,4,6,8,9,13,15,18	$2^{-6.5}$

Table 0.1968 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,10,17,18	2,4,6,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,10,16	2,4,6,8,9,11	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,10,17	2,4,6,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,10,16,18	2,4,6,8,9,11,15,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,10,14	2,4,6,8,9,11	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,10,14,16,17,18	2,4,6,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,10,14,18	2,4,6,8,9,11,15,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,10,14,16,17	2,4,6,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,10,17	2,4,6,8,9,11,13,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,10,16,18	2,4,6,8,9,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,10,17,18	2,4,6,8,9,11,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,10,16	2,4,6,8,9,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,10,14,18	2,4,6,8,9,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,10,14,16,17	2,4,6,8,9,11,13,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,10,14	2,4,6,8,9,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,10,14,16,17,18	2,4,6,8,9,11,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,10,12	2,4,6,8,9,11	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,10,12,16,17,18	2,4,6,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,10,12,18	2,4,6,8,9,11,15,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,10,12,16,17	2,4,6,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,10,12,14,17,18	2,4,6,8,9,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,10,12,14,16	2,4,6,8,9,11	2^{-1}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,10,12,14,17	2,4,6,8,9,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,10,12,14,16,18	2,4,6,8,9,11,15,18	2^{-1}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,10,12,18	2,4,6,8,9,11,13,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,10,12,16,17	2,4,6,8,9,11,13,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,10,12	2,4,6,8,9,11,13,15	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,10,12,16,17,18	2,4,6,8,9,11,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,10,12,14,17	2,4,6,8,9,11,13,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,10,12,14,16,18	2,4,6,8,9,11,13,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,10,12,14,17,18	2,4,6,8,9,11,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,10,12,14,16	2,4,6,8,9,11,13,15	$2^{-6.5}$

Table 0.1969 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,7,17	2,4,6,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,7,16,18	2,4,6,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,7,17,18	2,4,6,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,7,16	2,4,6,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,7,14,18	2,4,6,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,7,14,16,17	2,4,6,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,7,14	2,4,6,15	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0)$	1,3,7,14,16,17,18	2,4,6,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,7,17,18	2,4,6,13,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,7,16	2,4,6,13	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,7,17	2,4,6,13,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,7,16,18	2,4,6,13,15,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,7,14	2,4,6,13	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,7,14,16,17,18	2,4,6,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,7,14,18	2,4,6,13,15,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,7,14,16,17	2,4,6,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,7,12,18	2,4,6,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,7,12,16,17	2,4,6,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,7,12	2,4,6,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,7,12,16,17,18	2,4,6,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,7,12,14,17	2,4,6,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,7,12,14,16,18	2,4,6,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,7,12,14,17,18	2,4,6,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,7,12,14,16	2,4,6,15	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,7,12	2,4,6,13	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,7,12,16,17,18	2,4,6,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,7,12,18	2,4,6,13,15,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,7,12,16,17	2,4,6,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,7,12,14,17,18	2,4,6,13,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,7,12,14,16	2,4,6,13	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,7,12,14,17	2,4,6,13,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,7,12,14,16,18	2,4,6,13,15,18	2^{-23}

Table 0.1970 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,7,17,18	2,4,6,11,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,7,16	2,4,6,11	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,7,17	2,4,6,11,15,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,7,16,18	2,4,6,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,7,14	2,4,6,11	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,7,14,16,17,18	2,4,6,11,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,7,14,18	2,4,6,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,7,14,16,17	2,4,6,11,15,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,7,17	2,4,6,11,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,7,16,18	2,4,6,11,13,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,7,17,18	2,4,6,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,7,16	2,4,6,11,13,15	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,7,14,18	2,4,6,11,13,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,7,14,16,17	2,4,6,11,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,7,14	2,4,6,11,13,15	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,7,14,16,17,18	2,4,6,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,7,12	2,4,6,11	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,7,12,16,17,18	2,4,6,11,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,7,12,18	2,4,6,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,7,12,16,17	2,4,6,11,15,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,7,12,14,17,18	2,4,6,11,17,18	2^{-1}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,7,12,14,16	2,4,6,11	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,7,12,14,17	2,4,6,11,15,17	2^{-1}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,7,12,14,16,18	2,4,6,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,7,12,18	2,4,6,11,13,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,7,12,16,17	2,4,6,11,13,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,7,12	2,4,6,11,13,15	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,7,12,16,17,18	2,4,6,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,7,12,14,17	2,4,6,11,13,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,7,12,14,16,18	2,4,6,11,13,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,7,12,14,17,18	2,4,6,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,7,12,14,16	2,4,6,11,13,15	2^{-23}

Table 0.1971 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,7,10,18	2,4,6,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,7,10,16,17	2,4,6,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,7,10	2,4,6,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,7,10,16,17,18	2,4,6,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,7,10,14,17	2,4,6,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,7,10,14,16,18	2,4,6,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,7,10,14,17,18	2,4,6,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,7,10,14,16	2,4,6,15	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,7,10	2,4,6,13	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,7,10,16,17,18	2,4,6,13,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,7,10,18	2,4,6,13,15,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,7,10,16,17	2,4,6,13,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,7,10,14,17,18	2,4,6,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,7,10,14,16	2,4,6,13	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,7,10,14,17	2,4,6,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,7,10,14,16,18	2,4,6,13,15,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,7,10,12,17	2,4,6,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,7,10,12,16,18	2,4,6,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,7,10,12,17,18	2,4,6,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,7,10,12,16	2,4,6,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,7,10,12,14,18	2,4,6,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,7,10,12,14,16,17	2,4,6,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,7,10,12,14	2,4,6,15	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,7,10,12,14,16,17,18	2,4,6,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1)$	1,3,7,10,12,17,18	2,4,6,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,7,10,12,16	2,4,6,13	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,7,10,12,17	2,4,6,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,7,10,12,16,18	2,4,6,13,15,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,7,10,12,14	2,4,6,13	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,7,10,12,14,16,17,18	2,4,6,13,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,7,10,12,14,18	2,4,6,13,15,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,7,10,12,14,16,17	2,4,6,13,15,17	$2^{-28.5}$

Table 0.1972 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,7,10	2,4,6,11	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,7,10,16,17,18	2,4,6,11,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,7,10,18	2,4,6,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,7,10,16,17	2,4,6,11,15,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,7,10,14,17,18	2,4,6,11,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,7,10,14,16	2,4,6,11	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,7,10,14,17	2,4,6,11,15,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,7,10,14,16,18	2,4,6,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,7,10,18	2,4,6,11,13,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,7,10,16,17	2,4,6,11,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,7,10	2,4,6,11,13,15	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,7,10,16,17,18	2,4,6,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,7,10,14,17	2,4,6,11,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,7,10,14,16,18	2,4,6,11,13,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,7,10,14,17,18	2,4,6,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,7,10,14,16	2,4,6,11,13,15	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,7,10,12,17,18	2,4,6,11,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,7,10,12,16	2,4,6,11	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,7,10,12,17	2,4,6,11,15,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,7,10,12,16,18	2,4,6,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,7,10,12,14	2,4,6,11	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,7,10,12,14,16,17,18	2,4,6,11,17,18	2^{-34}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,7,10,12,14,18	2,4,6,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,7,10,12,14,16,17	2,4,6,11,15,17	2^{-34}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,7,10,12,17	2,4,6,11,13,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1)$	1,3,7,10,12,16,18	2,4,6,11,13,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,7,10,12,17,18	2,4,6,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,7,10,12,16	2,4,6,11,13,15	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,7,10,12,14,18	2,4,6,11,13,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,7,10,12,14,16,17	2,4,6,11,13,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,7,10,12,14	2,4,6,11,13,15	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,7,10,12,14,16,17,18	2,4,6,11,13,15,17,18	$2^{-28.5}$

Table 0.1973 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,7,17,18	2,4,6,9,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,7,16	2,4,6,9	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,7,17	2,4,6,9,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,7,16,18	2,4,6,9,15,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,7,14	2,4,6,9	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,7,14,16,17,18	2,4,6,9,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,7,14,18	2,4,6,9,15,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,7,14,16,17	2,4,6,9,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,7,17	2,4,6,9,13,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,7,16,18	2,4,6,9,13,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,7,17,18	2,4,6,9,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,7,16	2,4,6,9,13,15	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,7,14,18	2,4,6,9,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0)$	1,3,7,14,16,17	2,4,6,9,13,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,7,14	2,4,6,9,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,7,14,16,17,18	2,4,6,9,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,7,12	2,4,6,9	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,7,12,16,17,18	2,4,6,9,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,7,12,18	2,4,6,9,15,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,7,12,16,17	2,4,6,9,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,7,12,14,17,18	2,4,6,9,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,7,12,14,16	2,4,6,9	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,7,12,14,17	2,4,6,9,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,7,12,14,16,18	2,4,6,9,15,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,7,12,18	2,4,6,9,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,7,12,16,17	2,4,6,9,13,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,7,12	2,4,6,9,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,7,12,16,17,18	2,4,6,9,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,7,12,14,17	2,4,6,9,13,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,7,12,14,16,18	2,4,6,9,13,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,7,12,14,17,18	2,4,6,9,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,7,12,14,16	2,4,6,9,13,15	$2^{-28.5}$

Table 0.1974 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,7,17	2,4,6,9,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,7,16,18	2,4,6,9,11,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,7,17,18	2,4,6,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,7,16	2,4,6,9,11,15	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,7,14,18	2,4,6,9,11,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,7,14,16,17	2,4,6,9,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,7,14	2,4,6,9,11,15	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,7,14,16,17,18	2,4,6,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,7,17,18	2,4,6,9,11,13,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,7,16	2,4,6,9,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,7,17	2,4,6,9,11,13,15,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,7,16,18	2,4,6,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,7,14	2,4,6,9,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,7,14,16,17,18	2,4,6,9,11,13,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,7,14,18	2,4,6,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,7,14,16,17	2,4,6,9,11,13,15,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,7,12,18	2,4,6,9,11,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,7,12,16,17	2,4,6,9,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,7,12	2,4,6,9,11,15	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,7,12,16,17,18	2,4,6,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,7,12,14,17	2,4,6,9,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,7,12,14,16,18	2,4,6,9,11,18	2^{-34}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,7,12,14,17,18	2,4,6,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,7,12,14,16	2,4,6,9,11,15	2^{-34}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,7,12	2,4,6,9,11,13	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,7,12,16,17,18	2,4,6,9,11,13,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,7,12,18	2,4,6,9,11,13,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,7,12,16,17	2,4,6,9,11,13,15,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,7,12,14,17,18	2,4,6,9,11,13,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,7,12,14,16	2,4,6,9,11,13	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,7,12,14,17	2,4,6,9,11,13,15,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,7,12,14,16,18	2,4,6,9,11,13,15,18	$2^{-28.5}$

Table 0.1975 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,7,10	2,4,6,9	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,7,10,16,17,18	2,4,6,9,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,7,10,18	2,4,6,9,15,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,7,10,16,17	2,4,6,9,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,7,10,14,17,18	2,4,6,9,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,7,10,14,16	2,4,6,9	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,7,10,14,17	2,4,6,9,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,7,10,14,16,18	2,4,6,9,15,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,7,10,18	2,4,6,9,13,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,7,10,16,17	2,4,6,9,13,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0)$	1,3,7,10	2,4,6,9,13,15	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,7,10,16,17,18	2,4,6,9,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,7,10,14,17	2,4,6,9,13,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,7,10,14,16,18	2,4,6,9,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,7,10,14,17,18	2,4,6,9,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,7,10,14,16	2,4,6,9,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,7,10,12,17,18	2,4,6,9,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,7,10,12,16	2,4,6,9	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,7,10,12,17	2,4,6,9,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,7,10,12,16,18	2,4,6,9,15,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,7,10,12,14	2,4,6,9	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,7,10,12,14,16,17,18	2,4,6,9,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,7,10,12,14,18	2,4,6,9,15,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,7,10,12,14,16,17	2,4,6,9,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,10,12,17	2,4,6,9,13,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,7,10,12,16,18	2,4,6,9,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,10,12,17,18	2,4,6,9,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,7,10,12,16	2,4,6,9,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,7,10,12,14,18	2,4,6,9,13,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,7,10,12,14,16,17	2,4,6,9,13,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,7,10,12,14	2,4,6,9,13,15	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,7,10,12,14,16,17,18	2,4,6,9,13,15,17,18	2^{-23}

Table 0.1976 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,7,10,18	2,4,6,9,11,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,7,10,16,17	2,4,6,9,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,7,10	2,4,6,9,11,15	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,7,10,16,17,18	2,4,6,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,7,10,14,17	2,4,6,9,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,7,10,14,16,18	2,4,6,9,11,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,7,10,14,17,18	2,4,6,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,7,10,14,16	2,4,6,9,11,15	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,7,10	2,4,6,9,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,7,10,16,17,18	2,4,6,9,11,13,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,7,10,18	2,4,6,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,7,10,16,17	2,4,6,9,11,13,15,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,7,10,14,17,18	2,4,6,9,11,13,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,7,10,14,16	2,4,6,9,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,7,10,14,17	2,4,6,9,11,13,15,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,7,10,14,16,18	2,4,6,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,7,10,12,17	2,4,6,9,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,7,10,12,16,18	2,4,6,9,11,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,7,10,12,17,18	2,4,6,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,7,10,12,16	2,4,6,9,11,15	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,7,10,12,14,18	2,4,6,9,11,18	2^{-1}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,7,10,12,14,16,17	2,4,6,9,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,7,10,12,14	2,4,6,9,11,15	2^{-1}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,7,10,12,14,16,17,18	2,4,6,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,7,10,12,17,18	2,4,6,9,11,13,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,7,10,12,16	2,4,6,9,11,13	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,7,10,12,17	2,4,6,9,11,13,15,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,7,10,12,16,18	2,4,6,9,11,13,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,7,10,12,14	2,4,6,9,11,13	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,7,10,12,14,16,17,18	2,4,6,9,11,13,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,7,10,12,14,18	2,4,6,9,11,13,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,7,10,12,14,16,17	2,4,6,9,11,13,15,17	2^{-23}

Table 0.1977 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,7,18	2,4,6,8,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,7,16,17	2,4,6,8,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,7	2,4,6,8,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,7,16,17,18	2,4,6,8,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,7,14,17	2,4,6,8,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,7,14,16,18	2,4,6,8,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1)$	1,3,7,14,17,18	2,4,6,8,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,7,14,16	2,4,6,8,15	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,7	2,4,6,8,13	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,7,16,17,18	2,4,6,8,13,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,7,18	2,4,6,8,13,15,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,7,16,17	2,4,6,8,13,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,7,14,17,18	2,4,6,8,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,7,14,16	2,4,6,8,13	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,7,14,17	2,4,6,8,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,7,14,16,18	2,4,6,8,13,15,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,7,12,17	2,4,6,8,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,7,12,16,18	2,4,6,8,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,7,12,17,18	2,4,6,8,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,7,12,16	2,4,6,8,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,7,12,14,18	2,4,6,8,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,7,12,14,16,17	2,4,6,8,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,7,12,14	2,4,6,8,15	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,7,12,14,16,17,18	2,4,6,8,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,7,12,17,18	2,4,6,8,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,12,16	2,4,6,8,13	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,7,12,17	2,4,6,8,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,7,12,16,18	2,4,6,8,13,15,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,7,12,14	2,4,6,8,13	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,7,12,14,16,17,18	2,4,6,8,13,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,7,12,14,18	2,4,6,8,13,15,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,7,12,14,16,17	2,4,6,8,13,15,17	$2^{-6.5}$

Table 0.1978 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,7	2,4,6,8,11	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,7,16,17,18	2,4,6,8,11,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,7,18	2,4,6,8,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,7,16,17	2,4,6,8,11,15,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,7,14,17,18	2,4,6,8,11,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,7,14,16	2,4,6,8,11	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,7,14,17	2,4,6,8,11,15,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,7,14,16,18	2,4,6,8,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,7,18	2,4,6,8,11,13,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,7,16,17	2,4,6,8,11,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,7	2,4,6,8,11,13,15	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,7,16,17,18	2,4,6,8,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,7,14,17	2,4,6,8,11,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,7,14,16,18	2,4,6,8,11,13,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,7,14,17,18	2,4,6,8,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,7,14,16	2,4,6,8,11,13,15	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,7,12,17,18	2,4,6,8,11,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,7,12,16	2,4,6,8,11	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,7,12,17	2,4,6,8,11,15,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,7,12,16,18	2,4,6,8,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,7,12,14	2,4,6,8,11	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,7,12,14,16,17,18	2,4,6,8,11,17,18	2^{-1}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,7,12,14,18	2,4,6,8,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,7,12,14,16,17	2,4,6,8,11,15,17	2^{-1}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,7,12,17	2,4,6,8,11,13,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,7,12,16,18	2,4,6,8,11,13,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,7,12,17,18	2,4,6,8,11,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,7,12,16	2,4,6,8,11,13,15	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,7,12,14,18	2,4,6,8,11,13,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,7,12,14,16,17	2,4,6,8,11,13,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,7,12,14	2,4,6,8,11,13,15	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,7,12,14,16,17,18	2,4,6,8,11,13,15,17,18	$2^{-6.5}$

Table 0.1979 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,7,10,17	2,4,6,8,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,7,10,16,18	2,4,6,8,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,7,10,17,18	2,4,6,8,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,7,10,16	2,4,6,8,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,7,10,14,18	2,4,6,8,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,7,10,14,16,17	2,4,6,8,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,7,10,14	2,4,6,8,15	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,7,10,14,16,17,18	2,4,6,8,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,7,10,17,18	2,4,6,8,13,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,7,10,16	2,4,6,8,13	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,7,10,17	2,4,6,8,13,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,7,10,16,18	2,4,6,8,13,15,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,7,10,14	2,4,6,8,13	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,7,10,14,16,17,18	2,4,6,8,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,7,10,14,18	2,4,6,8,13,15,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,7,10,14,16,17	2,4,6,8,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,7,10,12,18	2,4,6,8,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,7,10,12,16,17	2,4,6,8,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,7,10,12	2,4,6,8,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,7,10,12,16,17,18	2,4,6,8,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,7,10,12,14,17	2,4,6,8,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,7,10,12,14,16,18	2,4,6,8,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,7,10,12,14,17,18	2,4,6,8,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1)$	1,3,7,10,12,14,16	2,4,6,8,15	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,7,10,12	2,4,6,8,13	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,7,10,12,16,17,18	2,4,6,8,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,7,10,12,18	2,4,6,8,13,15,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,7,10,12,16,17	2,4,6,8,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,7,10,12,14,17,18	2,4,6,8,13,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,7,10,12,14,16	2,4,6,8,13	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,7,10,12,14,17	2,4,6,8,13,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,7,10,12,14,16,18	2,4,6,8,13,15,18	2^{-12}

Table 0.1980 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,7,10,17,18	2,4,6,8,11,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,7,10,16	2,4,6,8,11	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,7,10,17	2,4,6,8,11,15,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,7,10,16,18	2,4,6,8,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,7,10,14	2,4,6,8,11	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,7,10,14,16,17,18	2,4,6,8,11,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,7,10,14,18	2,4,6,8,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,7,10,14,16,17	2,4,6,8,11,15,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,7,10,17	2,4,6,8,11,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,7,10,16,18	2,4,6,8,11,13,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,7,10,17,18	2,4,6,8,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,7,10,16	2,4,6,8,11,13,15	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,7,10,14,18	2,4,6,8,11,13,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,7,10,14,16,17	2,4,6,8,11,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,7,10,14	2,4,6,8,11,13,15	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,7,10,14,16,17,18	2,4,6,8,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,7,10,12	2,4,6,8,11	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,7,10,12,16,17,18	2,4,6,8,11,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,7,10,12,18	2,4,6,8,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,7,10,12,16,17	2,4,6,8,11,15,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,7,10,12,14,17,18	2,4,6,8,11,17,18	2^{-34}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,7,10,12,14,16	2,4,6,8,11	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,7,10,12,14,17	2,4,6,8,11,15,17	2^{-34}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,7,10,12,14,16,18	2,4,6,8,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,7,10,12,18	2,4,6,8,11,13,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,7,10,12,16,17	2,4,6,8,11,13,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,7,10,12	2,4,6,8,11,13,15	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,7,10,12,16,17,18	2,4,6,8,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,7,10,12,14,17	2,4,6,8,11,13,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,7,10,12,14,16,18	2,4,6,8,11,13,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,7,10,12,14,17,18	2,4,6,8,11,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,7,10,12,14,16	2,4,6,8,11,13,15	2^{-12}

Table 0.1981 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,7	2,4,6,8,9	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,7,16,17,18	2,4,6,8,9,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,7,18	2,4,6,8,9,15,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,7,16,17	2,4,6,8,9,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,7,14,17,18	2,4,6,8,9,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,7,14,16	2,4,6,8,9	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,7,14,17	2,4,6,8,9,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,7,14,16,18	2,4,6,8,9,15,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,7,18	2,4,6,8,9,13,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,7,16,17	2,4,6,8,9,13,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,7	2,4,6,8,9,13,15	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,7,16,17,18	2,4,6,8,9,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,7,14,17	2,4,6,8,9,13,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,7,14,16,18	2,4,6,8,9,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,7,14,17,18	2,4,6,8,9,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,7,14,16	2,4,6,8,9,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,7,12,17,18	2,4,6,8,9,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,7,12,16	2,4,6,8,9	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,7,12,17	2,4,6,8,9,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,7,12,16,18	2,4,6,8,9,15,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0)$	1,3,7,12,14	2,4,6,8,9	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,7,12,14,16,17,18	2,4,6,8,9,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,7,12,14,18	2,4,6,8,9,15,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0)$	1,3,7,12,14,16,17	2,4,6,8,9,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,7,12,17	2,4,6,8,9,13,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,7,12,16,18	2,4,6,8,9,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,7,12,17,18	2,4,6,8,9,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,7,12,16	2,4,6,8,9,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,7,12,14,18	2,4,6,8,9,13,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,7,12,14,16,17	2,4,6,8,9,13,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,7,12,14	2,4,6,8,9,13,15	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,7,12,14,16,17,18	2,4,6,8,9,13,15,17,18	2^{-12}

Table 0.1982 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,7,18	2,4,6,8,9,11,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,7,16,17	2,4,6,8,9,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,7	2,4,6,8,9,11,15	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,7,16,17,18	2,4,6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,7,14,17	2,4,6,8,9,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,7,14,16,18	2,4,6,8,9,11,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,7,14,17,18	2,4,6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,7,14,16	2,4,6,8,9,11,15	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,7	2,4,6,8,9,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,7,16,17,18	2,4,6,8,9,11,13,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,7,18	2,4,6,8,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,7,16,17	2,4,6,8,9,11,13,15,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,7,14,17,18	2,4,6,8,9,11,13,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,7,14,16	2,4,6,8,9,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,7,14,17	2,4,6,8,9,11,13,15,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,7,14,16,18	2,4,6,8,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,7,12,17	2,4,6,8,9,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,7,12,16,18	2,4,6,8,9,11,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,7,12,17,18	2,4,6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,7,12,16	2,4,6,8,9,11,15	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,7,12,14,18	2,4,6,8,9,11,18	2^{-34}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,7,12,14,16,17	2,4,6,8,9,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,7,12,14	2,4,6,8,9,11,15	2^{-34}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,7,12,14,16,17,18	2,4,6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,7,12,17,18	2,4,6,8,9,11,13,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,7,12,16	2,4,6,8,9,11,13	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,7,12,17	2,4,6,8,9,11,13,15,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,7,12,16,18	2,4,6,8,9,11,13,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,7,12,14	2,4,6,8,9,11,13	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,7,12,14,16,17,18	2,4,6,8,9,11,13,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,7,12,14,18	2,4,6,8,9,11,13,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,7,12,14,16,17	2,4,6,8,9,11,13,15,17	2^{-12}

Table 0.1983 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,7,10,17,18	2,4,6,8,9,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,7,10,16	2,4,6,8,9	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,7,10,17	2,4,6,8,9,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,7,10,16,18	2,4,6,8,9,15,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,7,10,14	2,4,6,8,9	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,7,10,14,16,17,18	2,4,6,8,9,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,7,10,14,18	2,4,6,8,9,15,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,7,10,14,16,17	2,4,6,8,9,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,7,10,17	2,4,6,8,9,13,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,7,10,16,18	2,4,6,8,9,13,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,7,10,17,18	2,4,6,8,9,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,7,10,16	2,4,6,8,9,13,15	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,7,10,14,18	2,4,6,8,9,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,7,10,14,16,17	2,4,6,8,9,13,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,7,10,14	2,4,6,8,9,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,7,10,14,16,17,18	2,4,6,8,9,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,7,10,12	2,4,6,8,9	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,7,10,12,16,17,18	2,4,6,8,9,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,7,10,12,18	2,4,6,8,9,15,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,7,10,12,16,17	2,4,6,8,9,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,7,10,12,14,17,18	2,4,6,8,9,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,7,10,12,14,16	2,4,6,8,9	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,7,10,12,14,17	2,4,6,8,9,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1)$	1,3,7,10,12,14,16,18	2,4,6,8,9,15,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,7,10,12,18	2,4,6,8,9,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,7,10,12,16,17	2,4,6,8,9,13,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,7,10,12	2,4,6,8,9,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,7,10,12,16,17,18	2,4,6,8,9,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,7,10,12,14,17	2,4,6,8,9,13,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,7,10,12,14,16,18	2,4,6,8,9,13,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,7,10,12,14,17,18	2,4,6,8,9,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,7,10,12,14,16	2,4,6,8,9,13,15	$2^{-6.5}$

Table 0.1984 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,7,10,17	2,4,6,8,9,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,7,10,16,18	2,4,6,8,9,11,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,7,10,17,18	2,4,6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,7,10,16	2,4,6,8,9,11,15	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,7,10,14,18	2,4,6,8,9,11,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,7,10,14,16,17	2,4,6,8,9,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,7,10,14	2,4,6,8,9,11,15	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,7,10,14,16,17,18	2,4,6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,7,10,17,18	2,4,6,8,9,11,13,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,7,10,16	2,4,6,8,9,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,7,10,17	2,4,6,8,9,11,13,15,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,7,10,16,18	2,4,6,8,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,7,10,14	2,4,6,8,9,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,7,10,14,16,17,18	2,4,6,8,9,11,13,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,7,10,14,18	2,4,6,8,9,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,7,10,14,16,17	2,4,6,8,9,11,13,15,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,7,10,12,18	2,4,6,8,9,11,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,7,10,12,16,17	2,4,6,8,9,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,7,10,12	2,4,6,8,9,11,15	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,7,10,12,16,17,18	2,4,6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,7,10,12,14,17	2,4,6,8,9,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,7,10,12,14,16,18	2,4,6,8,9,11,18	2^{-1}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,7,10,12,14,17,18	2,4,6,8,9,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,7,10,12,14,16	2,4,6,8,9,11,15	2^{-1}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,7,10,12	2,4,6,8,9,11,13	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,7,10,12,16,17,18	2,4,6,8,9,11,13,17,18	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,7,10,12,18	2,4,6,8,9,11,13,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,7,10,12,16,17	2,4,6,8,9,11,13,15,17	2^{-12}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,7,10,12,14,17,18	2,4,6,8,9,11,13,17,18	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,7,10,12,14,16	2,4,6,8,9,11,13	$2^{-6.5}$
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,7,10,12,14,17	2,4,6,8,9,11,13,15,17	2^{-23}
$(1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,7,10,12,14,16,18	2,4,6,8,9,11,13,15,18	$2^{-6.5}$

Table 0.1985 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,18	2,4,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,16,17	2,4,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,5	2,4,15	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,16,17,18	2,4,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,14,17	2,4,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,14,16,18	2,4,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,14,17,18	2,4,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,14,16	2,4,15	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,5	2,4,13	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,16,17,18	2,4,13,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,18	2,4,13,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,16,17	2,4,13,15,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,14,17,18	2,4,13,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,14,16	2,4,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,14,17	2,4,13,15,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,14,16,18	2,4,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,12,17	2,4,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,12,16,18	2,4,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,12,17,18	2,4,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,12,16	2,4,15	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,12,14,18	2,4,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,12,14,16,17	2,4,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,12,14	2,4,15	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,12,14,16,17,18	2,4,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,12,17,18	2,4,13,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,12,16	2,4,13	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,12,17	2,4,13,15,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,12,16,18	2,4,13,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,12,14	2,4,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,12,14,16,17,18	2,4,13,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,12,14,18	2,4,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,12,14,16,17	2,4,13,15,17	2^{-12}

Table 0.1986 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,5	2,4,11	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,16,17,18	2,4,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,18	2,4,11,15,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,16,17	2,4,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,14,17,18	2,4,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,14,16	2,4,11	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,14,17	2,4,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,14,16,18	2,4,11,15,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,18	2,4,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,16,17	2,4,11,13,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,5	2,4,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,16,17,18	2,4,11,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,14,17	2,4,11,13,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,14,16,18	2,4,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,14,17,18	2,4,11,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,14,16	2,4,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,12,17,18	2,4,11,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,12,16	2,4,11	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,12,17	2,4,11,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,12,16,18	2,4,11,15,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,12,14	2,4,11	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,12,14,16,17,18	2,4,11,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,12,14,18	2,4,11,15,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,12,14,16,17	2,4,11,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,12,17	2,4,11,13,17	2^{-1}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,12,16,18	2,4,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,12,17,18	2,4,11,13,15,17,18	2^{-1}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,12,16	2,4,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,12,14,18	2,4,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,12,14,16,17	2,4,11,13,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,12,14	2,4,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,12,14,16,17,18	2,4,11,13,15,17,18	2^{-12}

Table 0.1987 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,10,17	2,4,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,10,16,18	2,4,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,10,17,18	2,4,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,10,16	2,4,15	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,10,14,18	2,4,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,10,14,16,17	2,4,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,10,14	2,4,15	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,10,14,16,17,18	2,4,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,10,17,18	2,4,13,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,10,16	2,4,13	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,10,17	2,4,13,15,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,10,16,18	2,4,13,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,10,14	2,4,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,10,14,16,17,18	2,4,13,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,10,14,18	2,4,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,10,14,16,17	2,4,13,15,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,10,12,18	2,4,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,10,12,16,17	2,4,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,10,12	2,4,15	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,10,12,16,17,18	2,4,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,10,12,14,17	2,4,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,10,12,14,16,18	2,4,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,10,12,14,17,18	2,4,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,10,12,14,16	2,4,15	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,10,12	2,4,13	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,10,12,16,17,18	2,4,13,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,10,12,18	2,4,13,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,10,12,16,17	2,4,13,15,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,10,12,14,17,18	2,4,13,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,10,12,14,16	2,4,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,10,12,14,17	2,4,13,15,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,10,12,14,16,18	2,4,13,15,18	$2^{-17.5}$

Table 0.1988 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,10,17,18	2,4,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,10,16	2,4,11	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,10,17	2,4,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,10,16,18	2,4,11,15,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,10,14	2,4,11	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,10,14,16,17,18	2,4,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,10,14,18	2,4,11,15,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,10,14,16,17	2,4,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,10,17	2,4,11,13,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,10,16,18	2,4,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,10,17,18	2,4,11,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,10,16	2,4,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,10,14,18	2,4,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,10,14,16,17	2,4,11,13,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,10,14	2,4,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,10,14,16,17,18	2,4,11,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,10,12	2,4,11	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,10,12,16,17,18	2,4,11,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,10,12,18	2,4,11,15,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,10,12,16,17	2,4,11,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,10,12,14,17,18	2,4,11,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,10,12,14,16	2,4,11	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,10,12,14,17	2,4,11,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,10,12,14,16,18	2,4,11,15,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,10,12,18	2,4,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,10,12,16,17	2,4,11,13,17	2^{-34}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,10,12	2,4,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,10,12,16,17,18	2,4,11,13,15,17,18	2^{-34}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,10,12,14,17	2,4,11,13,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,10,12,14,16,18	2,4,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,10,12,14,17,18	2,4,11,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,10,12,14,16	2,4,11,13,15	$2^{-17.5}$

Table 0.1989 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,5	2,4,9	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,16,17,18	2,4,9,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,18	2,4,9,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,16,17	2,4,9,15,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,14,17,18	2,4,9,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,14,16	2,4,9	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,14,17	2,4,9,15,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,14,16,18	2,4,9,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,18	2,4,9,13,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,16,17	2,4,9,13,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5	2,4,9,13,15	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,16,17,18	2,4,9,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,14,17	2,4,9,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,14,16,18	2,4,9,13,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,14,17,18	2,4,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,14,16	2,4,9,13,15	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,12,17,18	2,4,9,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,12,16	2,4,9	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,12,17	2,4,9,15,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,12,16,18	2,4,9,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,12,14	2,4,9	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,12,14,16,17,18	2,4,9,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,12,14,18	2,4,9,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,12,14,16,17	2,4,9,15,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,12,17	2,4,9,13,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,12,16,18	2,4,9,13,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,12,17,18	2,4,9,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,12,16	2,4,9,13,15	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,12,14,18	2,4,9,13,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,12,14,16,17	2,4,9,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,12,14	2,4,9,13,15	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,12,14,16,17,18	2,4,9,13,15,17,18	$2^{-17.5}$

Table 0.1990 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,18	2,4,9,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,16,17	2,4,9,11,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,5	2,4,9,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,16,17,18	2,4,9,11,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,14,17	2,4,9,11,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,14,16,18	2,4,9,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,14,17,18	2,4,9,11,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,14,16	2,4,9,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,5	2,4,9,11,13	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,16,17,18	2,4,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,18	2,4,9,11,13,15,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,16,17	2,4,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,14,17,18	2,4,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,14,16	2,4,9,11,13	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,14,17	2,4,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,14,16,18	2,4,9,11,13,15,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,12,17	2,4,9,11,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,12,16,18	2,4,9,11,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,12,17,18	2,4,9,11,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,12,16	2,4,9,11,15	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,12,14,18	2,4,9,11,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,12,14,16,17	2,4,9,11,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,12,14	2,4,9,11,15	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,12,14,16,17,18	2,4,9,11,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,12,17,18	2,4,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,12,16	2,4,9,11,13	2^{-34}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,12,17	2,4,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,12,16,18	2,4,9,11,13,15,18	2^{-34}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,12,14	2,4,9,11,13	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,12,14,16,17,18	2,4,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,12,14,18	2,4,9,11,13,15,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,12,14,16,17	2,4,9,11,13,15,17	$2^{-17.5}$

Table 0.1991 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,10,17,18	2,4,9,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,10,16	2,4,9	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,10,17	2,4,9,15,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,10,16,18	2,4,9,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,10,14	2,4,9	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,10,14,16,17,18	2,4,9,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,10,14,18	2,4,9,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,10,14,16,17	2,4,9,15,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,10,17	2,4,9,13,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,10,16,18	2,4,9,13,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,10,17,18	2,4,9,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,10,16	2,4,9,13,15	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,10,14,18	2,4,9,13,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,10,14,16,17	2,4,9,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,10,14	2,4,9,13,15	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,10,14,16,17,18	2,4,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,10,12	2,4,9	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,10,12,16,17,18	2,4,9,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,10,12,18	2,4,9,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,10,12,16,17	2,4,9,15,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,10,12,14,17,18	2,4,9,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,10,12,14,16	2,4,9	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,10,12,14,17	2,4,9,15,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,10,12,14,16,18	2,4,9,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,10,12,18	2,4,9,13,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,10,12,16,17	2,4,9,13,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,10,12	2,4,9,13,15	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,10,12,16,17,18	2,4,9,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,10,12,14,17	2,4,9,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,10,12,14,16,18	2,4,9,13,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,10,12,14,17,18	2,4,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,10,12,14,16	2,4,9,13,15	2^{-12}

Table 0.1992 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,10,17	2,4,9,11,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,10,16,18	2,4,9,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,10,17,18	2,4,9,11,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,10,16	2,4,9,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,10,14,18	2,4,9,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,10,14,16,17	2,4,9,11,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,10,14	2,4,9,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,10,14,16,17,18	2,4,9,11,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,10,17,18	2,4,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,10,16	2,4,9,11,13	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,10,17	2,4,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,10,16,18	2,4,9,11,13,15,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,10,14	2,4,9,11,13	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,10,14,16,17,18	2,4,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,10,14,18	2,4,9,11,13,15,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,10,14,16,17	2,4,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,10,12,18	2,4,9,11,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,10,12,16,17	2,4,9,11,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,10,12	2,4,9,11,15	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,10,12,16,17,18	2,4,9,11,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,10,12,14,17	2,4,9,11,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,10,12,14,16,18	2,4,9,11,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,10,12,14,17,18	2,4,9,11,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,10,12,14,16	2,4,9,11,15	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,10,12	2,4,9,11,13	2^{-1}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,10,12,16,17,18	2,4,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,10,12,18	2,4,9,11,13,15,18	2^{-1}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,10,12,16,17	2,4,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,10,12,14,17,18	2,4,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,10,12,14,16	2,4,9,11,13	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,10,12,14,17	2,4,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,10,12,14,16,18	2,4,9,11,13,15,18	2^{-12}

Table 0.1993 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,17	2,4,8,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,16,18	2,4,8,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,17,18	2,4,8,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,16	2,4,8,15	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,14,18	2,4,8,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,14,16,17	2,4,8,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,14	2,4,8,15	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,14,16,17,18	2,4,8,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,17,18	2,4,8,13,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,16	2,4,8,13	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,17	2,4,8,13,15,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,16,18	2,4,8,13,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,14	2,4,8,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,14,16,17,18	2,4,8,13,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,14,18	2,4,8,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,14,16,17	2,4,8,13,15,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,12,18	2,4,8,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,12,16,17	2,4,8,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,12	2,4,8,15	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,12,16,17,18	2,4,8,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,12,14,17	2,4,8,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,12,14,16,18	2,4,8,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,12,14,17,18	2,4,8,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,12,14,16	2,4,8,15	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,12	2,4,8,13	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,12,16,17,18	2,4,8,13,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,12,18	2,4,8,13,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,12,16,17	2,4,8,13,15,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,12,14,17,18	2,4,8,13,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,12,14,16	2,4,8,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,12,14,17	2,4,8,13,15,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,12,14,16,18	2,4,8,13,15,18	$2^{-17.5}$

Table 0.1994 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,17,18	2,4,8,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,16	2,4,8,11	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,17	2,4,8,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,16,18	2,4,8,11,15,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,14	2,4,8,11	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,14,16,17,18	2,4,8,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,14,18	2,4,8,11,15,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,14,16,17	2,4,8,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,17	2,4,8,11,13,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,16,18	2,4,8,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,17,18	2,4,8,11,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,16	2,4,8,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,14,18	2,4,8,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,14,16,17	2,4,8,11,13,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,14	2,4,8,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,14,16,17,18	2,4,8,11,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,12	2,4,8,11	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,12,16,17,18	2,4,8,11,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,12,18	2,4,8,11,15,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,12,16,17	2,4,8,11,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,12,14,17,18	2,4,8,11,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,12,14,16	2,4,8,11	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,12,14,17	2,4,8,11,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,12,14,16,18	2,4,8,11,15,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,12,18	2,4,8,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,12,16,17	2,4,8,11,13,17	2^{-1}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,12	2,4,8,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,12,16,17,18	2,4,8,11,13,15,17,18	2^{-1}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,12,14,17	2,4,8,11,13,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,12,14,16,18	2,4,8,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,12,14,17,18	2,4,8,11,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,12,14,16	2,4,8,11,13,15	$2^{-17.5}$

Table 0.1995 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,10,18	2,4,8,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,10,16,17	2,4,8,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,10	2,4,8,15	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,10,16,17,18	2,4,8,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,10,14,17	2,4,8,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,10,14,16,18	2,4,8,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,10,14,17,18	2,4,8,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,10,14,16	2,4,8,15	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,10	2,4,8,13	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,10,16,17,18	2,4,8,13,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,10,18	2,4,8,13,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,10,16,17	2,4,8,13,15,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,10,14,17,18	2,4,8,13,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,10,14,16	2,4,8,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,10,14,17	2,4,8,13,15,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,10,14,16,18	2,4,8,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,10,12,17	2,4,8,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,10,12,16,18	2,4,8,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,10,12,17,18	2,4,8,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,10,12,16	2,4,8,15	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,10,12,14,18	2,4,8,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,10,12,14,16,17	2,4,8,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,10,12,14	2,4,8,15	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,10,12,14,16,17,18	2,4,8,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,10,12,17,18	2,4,8,13,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,10,12,16	2,4,8,13	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,10,12,17	2,4,8,13,15,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,10,12,16,18	2,4,8,13,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,10,12,14	2,4,8,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,10,12,14,16,17,18	2,4,8,13,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,10,12,14,18	2,4,8,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,10,12,14,16,17	2,4,8,13,15,17	2^{-23}

Table 0.1996 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,10	2,4,8,11	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,10,16,17,18	2,4,8,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,10,18	2,4,8,11,15,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,10,16,17	2,4,8,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,10,14,17,18	2,4,8,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,10,14,16	2,4,8,11	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,10,14,17	2,4,8,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,10,14,16,18	2,4,8,11,15,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,10,18	2,4,8,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,10,16,17	2,4,8,11,13,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,10	2,4,8,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,10,16,17,18	2,4,8,11,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,10,14,17	2,4,8,11,13,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,10,14,16,18	2,4,8,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,10,14,17,18	2,4,8,11,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,10,14,16	2,4,8,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,10,12,17,18	2,4,8,11,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,10,12,16	2,4,8,11	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,10,12,17	2,4,8,11,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,10,12,16,18	2,4,8,11,15,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,10,12,14	2,4,8,11	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,10,12,14,16,17,18	2,4,8,11,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,10,12,14,18	2,4,8,11,15,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,10,12,14,16,17	2,4,8,11,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,10,12,17	2,4,8,11,13,17	2^{-34}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,10,12,16,18	2,4,8,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,10,12,17,18	2,4,8,11,13,15,17,18	2^{-34}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,10,12,16	2,4,8,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,10,12,14,18	2,4,8,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,10,12,14,16,17	2,4,8,11,13,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,10,12,14	2,4,8,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,10,12,14,16,17,18	2,4,8,11,13,15,17,18	2^{-23}

Table 0.1997 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,17,18	2,4,8,9,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,16	2,4,8,9	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,17	2,4,8,9,15,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,16,18	2,4,8,9,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,14	2,4,8,9	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,14,16,17,18	2,4,8,9,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,14,18	2,4,8,9,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,14,16,17	2,4,8,9,15,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,17	2,4,8,9,13,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,16,18	2,4,8,9,13,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,17,18	2,4,8,9,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,16	2,4,8,9,13,15	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,14,18	2,4,8,9,13,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,14,16,17	2,4,8,9,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,14	2,4,8,9,13,15	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,14,16,17,18	2,4,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,12	2,4,8,9	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,12,16,17,18	2,4,8,9,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,12,18	2,4,8,9,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,12,16,17	2,4,8,9,15,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,12,14,17,18	2,4,8,9,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,12,14,16	2,4,8,9	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,12,14,17	2,4,8,9,15,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,12,14,16,18	2,4,8,9,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,12,18	2,4,8,9,13,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,12,16,17	2,4,8,9,13,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,12	2,4,8,9,13,15	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,12,16,17,18	2,4,8,9,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,12,14,17	2,4,8,9,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,12,14,16,18	2,4,8,9,13,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,12,14,17,18	2,4,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,12,14,16	2,4,8,9,13,15	2^{-23}

Table 0.1998 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,17	2,4,8,9,11,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,16,18	2,4,8,9,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,17,18	2,4,8,9,11,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,16	2,4,8,9,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,14,18	2,4,8,9,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,14,16,17	2,4,8,9,11,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,14	2,4,8,9,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,14,16,17,18	2,4,8,9,11,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,17,18	2,4,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,16	2,4,8,9,11,13	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,17	2,4,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,16,18	2,4,8,9,11,13,15,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,14	2,4,8,9,11,13	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,14,16,17,18	2,4,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,14,18	2,4,8,9,11,13,15,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,14,16,17	2,4,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,12,18	2,4,8,9,11,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,12,16,17	2,4,8,9,11,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,12	2,4,8,9,11,15	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,12,16,17,18	2,4,8,9,11,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,12,14,17	2,4,8,9,11,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,12,14,16,18	2,4,8,9,11,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,12,14,17,18	2,4,8,9,11,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,12,14,16	2,4,8,9,11,15	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,12	2,4,8,9,11,13	2^{-34}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,12,16,17,18	2,4,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,12,18	2,4,8,9,11,13,15,18	2^{-34}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,12,16,17	2,4,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,12,14,17,18	2,4,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,12,14,16	2,4,8,9,11,13	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,12,14,17	2,4,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,12,14,16,18	2,4,8,9,11,13,15,18	2^{-23}

Table 0.1999 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,10	2,4,8,9	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,10,16,17,18	2,4,8,9,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,10,18	2,4,8,9,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,10,16,17	2,4,8,9,15,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,10,14,17,18	2,4,8,9,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,10,14,16	2,4,8,9	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,10,14,17	2,4,8,9,15,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,10,14,16,18	2,4,8,9,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,10,18	2,4,8,9,13,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,10,16,17	2,4,8,9,13,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,10	2,4,8,9,13,15	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,10,16,17,18	2,4,8,9,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,10,14,17	2,4,8,9,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,10,14,16,18	2,4,8,9,13,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,10,14,17,18	2,4,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,10,14,16	2,4,8,9,13,15	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,10,12,17,18	2,4,8,9,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,10,12,16	2,4,8,9	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,10,12,17	2,4,8,9,15,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,10,12,16,18	2,4,8,9,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,10,12,14	2,4,8,9	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,10,12,14,16,17,18	2,4,8,9,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,10,12,14,18	2,4,8,9,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,10,12,14,16,17	2,4,8,9,15,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,10,12,17	2,4,8,9,13,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,10,12,16,18	2,4,8,9,13,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,10,12,17,18	2,4,8,9,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,10,12,16	2,4,8,9,13,15	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,10,12,14,18	2,4,8,9,13,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,10,12,14,16,17	2,4,8,9,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,10,12,14	2,4,8,9,13,15	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,10,12,14,16,17,18	2,4,8,9,13,15,17,18	$2^{-17.5}$

Table 0.2000 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,10,18	2,4,8,9,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,10,16,17	2,4,8,9,11,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,10	2,4,8,9,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,10,16,17,18	2,4,8,9,11,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,10,14,17	2,4,8,9,11,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,10,14,16,18	2,4,8,9,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,10,14,17,18	2,4,8,9,11,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,10,14,16	2,4,8,9,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,10	2,4,8,9,11,13	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,10,16,17,18	2,4,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,10,18	2,4,8,9,11,13,15,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,10,16,17	2,4,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,10,14,17,18	2,4,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,10,14,16	2,4,8,9,11,13	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,10,14,17	2,4,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,10,14,16,18	2,4,8,9,11,13,15,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,10,12,17	2,4,8,9,11,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,10,12,16,18	2,4,8,9,11,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,10,12,17,18	2,4,8,9,11,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,10,12,16	2,4,8,9,11,15	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,10,12,14,18	2,4,8,9,11,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,10,12,14,16,17	2,4,8,9,11,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,10,12,14	2,4,8,9,11,15	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,10,12,14,16,17,18	2,4,8,9,11,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,10,12,17,18	2,4,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,10,12,16	2,4,8,9,11,13	2^{-1}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,10,12,17	2,4,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,10,12,16,18	2,4,8,9,11,13,15,18	2^{-1}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,10,12,14	2,4,8,9,11,13	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,10,12,14,16,17,18	2,4,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,10,12,14,18	2,4,8,9,11,13,15,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,10,12,14,16,17	2,4,8,9,11,13,15,17	$2^{-17.5}$

Table 0.2001 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,7	2,4	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,16,17,18	2,4,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,7,18	2,4,15,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,16,17	2,4,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,14,17,18	2,4,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,7,14,16	2,4	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,14,17	2,4,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,7,14,16,18	2,4,15,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,7,18	2,4,13,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,7,16,17	2,4,13,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,7	2,4,13,15	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,7,16,17,18	2,4,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,7,14,17	2,4,13,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,7,14,16,18	2,4,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,7,14,17,18	2,4,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,7,14,16	2,4,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,12,17,18	2,4,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,7,12,16	2,4	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,12,17	2,4,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,7,12,16,18	2,4,15,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,7,12,14	2,4	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,7,12,14,16,17,18	2,4,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,7,12,14,18	2,4,15,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,7,12,14,16,17	2,4,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,12,17	2,4,13,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,7,12,16,18	2,4,13,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,12,17,18	2,4,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,7,12,16	2,4,13,15	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,7,12,14,18	2,4,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,12,14,16,17	2,4,13,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,7,12,14	2,4,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,12,14,16,17,18	2,4,13,15,17,18	2^{-12}

Table 0.2002 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,18	2,4,11,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,7,16,17	2,4,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,7	2,4,11,15	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,7,16,17,18	2,4,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,7,14,17	2,4,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,7,14,16,18	2,4,11,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,7,14,17,18	2,4,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,7,14,16	2,4,11,15	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7	2,4,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,7,16,17,18	2,4,11,13,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,18	2,4,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,7,16,17	2,4,11,13,15,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,7,14,17,18	2,4,11,13,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,7,14,16	2,4,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,7,14,17	2,4,11,13,15,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,7,14,16,18	2,4,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,7,12,17	2,4,11,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,7,12,16,18	2,4,11,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,7,12,17,18	2,4,11,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,7,12,16	2,4,11,15	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,7,12,14,18	2,4,11,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,7,12,14,16,17	2,4,11,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,7,12,14	2,4,11,15	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,7,12,14,16,17,18	2,4,11,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,7,12,17,18	2,4,11,13,17,18	2^{-1}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,7,12,16	2,4,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,7,12,17	2,4,11,13,15,17	2^{-1}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,7,12,16,18	2,4,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,7,12,14	2,4,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,7,12,14,16,17,18	2,4,11,13,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,7,12,14,18	2,4,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,7,12,14,16,17	2,4,11,13,15,17	2^{-12}

Table 0.2003 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,7,10,17,18	2,4,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,7,10,16	2,4	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,7,10,17	2,4,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,7,10,16,18	2,4,15,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,7,10,14	2,4	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,7,10,14,16,17,18	2,4,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,7,10,14,18	2,4,15,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,7,10,14,16,17	2,4,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,7,10,17	2,4,13,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,7,10,16,18	2,4,13,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,7,10,17,18	2,4,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,7,10,16	2,4,13,15	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,7,10,14,18	2,4,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,7,10,14,16,17	2,4,13,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,7,10,14	2,4,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,7,10,14,16,17,18	2,4,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,7,10,12	2,4	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,7,10,12,16,17,18	2,4,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,7,10,12,18	2,4,15,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,7,10,12,16,17	2,4,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,7,10,12,14,17,18	2,4,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,7,10,12,14,16	2,4	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,7,10,12,14,17	2,4,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,7,10,12,14,16,18	2,4,15,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,7,10,12,18	2,4,13,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,7,10,12,16,17	2,4,13,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,7,10,12	2,4,13,15	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,7,10,12,16,17,18	2,4,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,7,10,12,14,17	2,4,13,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,7,10,12,14,16,18	2,4,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,10,12,14,17,18	2,4,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,7,10,12,14,16	2,4,13,15	$2^{-17.5}$

Table 0.2004 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,7,10,17	2,4,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,7,10,16,18	2,4,11,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,7,10,17,18	2,4,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,7,10,16	2,4,11,15	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,7,10,14,18	2,4,11,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,7,10,14,16,17	2,4,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,7,10,14	2,4,11,15	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,7,10,14,16,17,18	2,4,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,7,10,17,18	2,4,11,13,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,7,10,16	2,4,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,7,10,17	2,4,11,13,15,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,7,10,16,18	2,4,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,7,10,14	2,4,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,7,10,14,16,17,18	2,4,11,13,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,7,10,14,18	2,4,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,7,10,14,16,17	2,4,11,13,15,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,7,10,12,18	2,4,11,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,7,10,12,16,17	2,4,11,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,7,10,12	2,4,11,15	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,7,10,12,16,17,18	2,4,11,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,7,10,12,14,17	2,4,11,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,7,10,12,14,16,18	2,4,11,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,7,10,12,14,17,18	2,4,11,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,7,10,12,14,16	2,4,11,15	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,7,10,12	2,4,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7,10,12,16,17,18	2,4,11,13,17,18	2^{-34}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,7,10,12,18	2,4,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7,10,12,16,17	2,4,11,13,15,17	2^{-34}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,7,10,12,14,17,18	2,4,11,13,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,7,10,12,14,16	2,4,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,7,10,12,14,17	2,4,11,13,15,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,7,10,12,14,16,18	2,4,11,13,15,18	$2^{-17.5}$

Table 0.2005 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,7,18	2,4,9,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,7,16,17	2,4,9,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,7	2,4,9,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,7,16,17,18	2,4,9,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,7,14,17	2,4,9,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,7,14,16,18	2,4,9,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,7,14,17,18	2,4,9,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,7,14,16	2,4,9,15	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,7	2,4,9,13	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,7,16,17,18	2,4,9,13,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,7,18	2,4,9,13,15,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,7,16,17	2,4,9,13,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,7,14,17,18	2,4,9,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,7,14,16	2,4,9,13	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,7,14,17	2,4,9,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,7,14,16,18	2,4,9,13,15,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,7,12,17	2,4,9,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,7,12,16,18	2,4,9,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,7,12,17,18	2,4,9,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,7,12,16	2,4,9,15	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,7,12,14,18	2,4,9,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,7,12,14,16,17	2,4,9,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,7,12,14	2,4,9,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,7,12,14,16,17,18	2,4,9,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,7,12,17,18	2,4,9,13,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,7,12,16	2,4,9,13	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,7,12,17	2,4,9,13,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,7,12,16,18	2,4,9,13,15,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,7,12,14	2,4,9,13	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,7,12,14,16,17,18	2,4,9,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,12,14,18	2,4,9,13,15,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,7,12,14,16,17	2,4,9,13,15,17	$2^{-17.5}$

Table 0.2006 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,7	2,4,9,11	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,7,16,17,18	2,4,9,11,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,7,18	2,4,9,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,7,16,17	2,4,9,11,15,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,7,14,17,18	2,4,9,11,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,7,14,16	2,4,9,11	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,7,14,17	2,4,9,11,15,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,7,14,16,18	2,4,9,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,7,18	2,4,9,11,13,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,7,16,17	2,4,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,7	2,4,9,11,13,15	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,7,16,17,18	2,4,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,7,14,17	2,4,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,7,14,16,18	2,4,9,11,13,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,7,14,17,18	2,4,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,7,14,16	2,4,9,11,13,15	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,7,12,17,18	2,4,9,11,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,7,12,16	2,4,9,11	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,7,12,17	2,4,9,11,15,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,7,12,16,18	2,4,9,11,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,7,12,14	2,4,9,11	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,7,12,14,16,17,18	2,4,9,11,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,7,12,14,18	2,4,9,11,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,7,12,14,16,17	2,4,9,11,15,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,7,12,17	2,4,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,7,12,16,18	2,4,9,11,13,18	2^{-34}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,7,12,17,18	2,4,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,7,12,16	2,4,9,11,13,15	2^{-34}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,7,12,14,18	2,4,9,11,13,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,7,12,14,16,17	2,4,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,7,12,14	2,4,9,11,13,15	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,7,12,14,16,17,18	2,4,9,11,13,15,17,18	$2^{-17.5}$

Table 0.2007 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,7,10,17	2,4,9,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,7,10,16,18	2,4,9,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,7,10,17,18	2,4,9,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,7,10,16	2,4,9,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,7,10,14,18	2,4,9,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,7,10,14,16,17	2,4,9,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,7,10,14	2,4,9,15	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,7,10,14,16,17,18	2,4,9,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,7,10,17,18	2,4,9,13,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,7,10,16	2,4,9,13	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,7,10,17	2,4,9,13,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,7,10,16,18	2,4,9,13,15,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,7,10,14	2,4,9,13	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,7,10,14,16,17,18	2,4,9,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,7,10,14,18	2,4,9,13,15,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,7,10,14,16,17	2,4,9,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10,12,18	2,4,9,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,12,16,17	2,4,9,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10,12	2,4,9,15	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,12,16,17,18	2,4,9,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,7,10,12,14,17	2,4,9,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,7,10,12,14,16,18	2,4,9,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,7,10,12,14,17,18	2,4,9,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,7,10,12,14,16	2,4,9,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10,12	2,4,9,13	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,12,16,17,18	2,4,9,13,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10,12,18	2,4,9,13,15,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,12,16,17	2,4,9,13,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,7,10,12,14,17,18	2,4,9,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,7,10,12,14,16	2,4,9,13	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,7,10,12,14,17	2,4,9,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,7,10,12,14,16,18	2,4,9,13,15,18	2^{-12}

Table 0.2008 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,7,10,17,18	2,4,9,11,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,7,10,16	2,4,9,11	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,7,10,17	2,4,9,11,15,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,7,10,16,18	2,4,9,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,7,10,14	2,4,9,11	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,7,10,14,16,17,18	2,4,9,11,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,7,10,14,18	2,4,9,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,7,10,14,16,17	2,4,9,11,15,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,7,10,17	2,4,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,7,10,16,18	2,4,9,11,13,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,7,10,17,18	2,4,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,7,10,16	2,4,9,11,13,15	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,10,14,18	2,4,9,11,13,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,7,10,14,16,17	2,4,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,10,14	2,4,9,11,13,15	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,7,10,14,16,17,18	2,4,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,7,10,12	2,4,9,11	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7,10,12,16,17,18	2,4,9,11,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,7,10,12,18	2,4,9,11,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7,10,12,16,17	2,4,9,11,15,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,7,10,12,14,17,18	2,4,9,11,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,7,10,12,14,16	2,4,9,11	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,7,10,12,14,17	2,4,9,11,15,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,7,10,12,14,16,18	2,4,9,11,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,7,10,12,18	2,4,9,11,13,18	2^{-1}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,7,10,12,16,17	2,4,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,7,10,12	2,4,9,11,13,15	2^{-1}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,7,10,12,16,17,18	2,4,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,7,10,12,14,17	2,4,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,7,10,12,14,16,18	2,4,9,11,13,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,7,10,12,14,17,18	2,4,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,7,10,12,14,16	2,4,9,11,13,15	2^{-12}

Table 0.2009 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,7,17,18	2,4,8,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,7,16	2,4,8	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,7,17	2,4,8,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,7,16,18	2,4,8,15,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,7,14	2,4,8	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,7,14,16,17,18	2,4,8,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,7,14,18	2,4,8,15,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,7,14,16,17	2,4,8,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,7,17	2,4,8,13,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,7,16,18	2,4,8,13,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,7,17,18	2,4,8,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,7,16	2,4,8,13,15	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,7,14,18	2,4,8,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,7,14,16,17	2,4,8,13,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,7,14	2,4,8,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,7,14,16,17,18	2,4,8,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,7,12	2,4,8	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,7,12,16,17,18	2,4,8,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,7,12,18	2,4,8,15,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,7,12,16,17	2,4,8,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,7,12,14,17,18	2,4,8,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,7,12,14,16	2,4,8	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,7,12,14,17	2,4,8,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,7,12,14,16,18	2,4,8,15,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,7,12,18	2,4,8,13,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,7,12,16,17	2,4,8,13,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,7,12	2,4,8,13,15	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,7,12,16,17,18	2,4,8,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,7,12,14,17	2,4,8,13,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,7,12,14,16,18	2,4,8,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,7,12,14,17,18	2,4,8,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,7,12,14,16	2,4,8,13,15	$2^{-17.5}$

Table 0.2010 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,7,17	2,4,8,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,7,16,18	2,4,8,11,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,7,17,18	2,4,8,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,7,16	2,4,8,11,15	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,7,14,18	2,4,8,11,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,7,14,16,17	2,4,8,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,7,14	2,4,8,11,15	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,7,14,16,17,18	2,4,8,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,7,17,18	2,4,8,11,13,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,7,16	2,4,8,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,7,17	2,4,8,11,13,15,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,7,16,18	2,4,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,7,14	2,4,8,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,7,14,16,17,18	2,4,8,11,13,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,7,14,18	2,4,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,14,16,17	2,4,8,11,13,15,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7,12,18	2,4,8,11,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,7,12,16,17	2,4,8,11,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7,12	2,4,8,11,15	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,7,12,16,17,18	2,4,8,11,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,7,12,14,17	2,4,8,11,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,7,12,14,16,18	2,4,8,11,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,7,12,14,17,18	2,4,8,11,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,7,12,14,16	2,4,8,11,15	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,7,12	2,4,8,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,7,12,16,17,18	2,4,8,11,13,17,18	2^{-1}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,7,12,18	2,4,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,7,12,16,17	2,4,8,11,13,15,17	2^{-1}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,7,12,14,17,18	2,4,8,11,13,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,7,12,14,16	2,4,8,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,7,12,14,17	2,4,8,11,13,15,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,7,12,14,16,18	2,4,8,11,13,15,18	$2^{-17.5}$

Table 0.2011 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,7,10	2,4,8	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,7,10,16,17,18	2,4,8,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,7,10,18	2,4,8,15,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,16,17	2,4,8,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,7,10,14,17,18	2,4,8,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,7,10,14,16	2,4,8	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,7,10,14,17	2,4,8,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,7,10,14,16,18	2,4,8,15,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,7,10,18	2,4,8,13,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,7,10,16,17	2,4,8,13,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,7,10	2,4,8,13,15	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,7,10,16,17,18	2,4,8,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,7,10,14,17	2,4,8,13,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,7,10,14,16,18	2,4,8,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,7,10,14,17,18	2,4,8,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,7,10,14,16	2,4,8,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,7,10,12,17,18	2,4,8,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,7,10,12,16	2,4,8	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,7,10,12,17	2,4,8,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,7,10,12,16,18	2,4,8,15,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,7,10,12,14	2,4,8	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,7,10,12,14,16,17,18	2,4,8,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,7,10,12,14,18	2,4,8,15,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,7,10,12,14,16,17	2,4,8,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,7,10,12,17	2,4,8,13,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,7,10,12,16,18	2,4,8,13,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,7,10,12,17,18	2,4,8,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,7,10,12,16	2,4,8,13,15	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,7,10,12,14,18	2,4,8,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,7,10,12,14,16,17	2,4,8,13,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,7,10,12,14	2,4,8,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,7,10,12,14,16,17,18	2,4,8,13,15,17,18	2^{-23}

Table 0.2012 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,7,10,18	2,4,8,11,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,7,10,16,17	2,4,8,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,7,10	2,4,8,11,15	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,7,10,16,17,18	2,4,8,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,7,10,14,17	2,4,8,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,7,10,14,16,18	2,4,8,11,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,7,10,14,17,18	2,4,8,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,7,10,14,16	2,4,8,11,15	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,7,10	2,4,8,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,7,10,16,17,18	2,4,8,11,13,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,7,10,18	2,4,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,7,10,16,17	2,4,8,11,13,15,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,7,10,14,17,18	2,4,8,11,13,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,7,10,14,16	2,4,8,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,7,10,14,17	2,4,8,11,13,15,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,7,10,14,16,18	2,4,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,7,10,12,17	2,4,8,11,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,7,10,12,16,18	2,4,8,11,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,7,10,12,17,18	2,4,8,11,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,7,10,12,16	2,4,8,11,15	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,7,10,12,14,18	2,4,8,11,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,7,10,12,14,16,17	2,4,8,11,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,7,10,12,14	2,4,8,11,15	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,7,10,12,14,16,17,18	2,4,8,11,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,7,10,12,17,18	2,4,8,11,13,17,18	2^{-34}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,7,10,12,16	2,4,8,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,7,10,12,17	2,4,8,11,13,15,17	2^{-34}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,7,10,12,16,18	2,4,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,7,10,12,14	2,4,8,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,7,10,12,14,16,17,18	2,4,8,11,13,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,7,10,12,14,18	2,4,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,7,10,12,14,16,17	2,4,8,11,13,15,17	2^{-23}

Table 0.2013 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,7,17	2,4,8,9,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,7,16,18	2,4,8,9,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,7,17,18	2,4,8,9,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,7,16	2,4,8,9,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,7,14,18	2,4,8,9,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,7,14,16,17	2,4,8,9,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,7,14	2,4,8,9,15	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,7,14,16,17,18	2,4,8,9,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,7,17,18	2,4,8,9,13,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,7,16	2,4,8,9,13	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,7,17	2,4,8,9,13,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,7,16,18	2,4,8,9,13,15,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,7,14	2,4,8,9,13	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,7,14,16,17,18	2,4,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,7,14,18	2,4,8,9,13,15,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,7,14,16,17	2,4,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,7,12,18	2,4,8,9,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,7,12,16,17	2,4,8,9,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,7,12	2,4,8,9,15	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,7,12,16,17,18	2,4,8,9,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,7,12,14,17	2,4,8,9,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,7,12,14,16,18	2,4,8,9,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,7,12,14,17,18	2,4,8,9,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,7,12,14,16	2,4,8,9,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,7,12	2,4,8,9,13	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,7,12,16,17,18	2,4,8,9,13,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,7,12,18	2,4,8,9,13,15,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,7,12,16,17	2,4,8,9,13,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,7,12,14,17,18	2,4,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,7,12,14,16	2,4,8,9,13	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,7,12,14,17	2,4,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,7,12,14,16,18	2,4,8,9,13,15,18	2^{-23}

Table 0.2014 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,7,17,18	2,4,8,9,11,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,7,16	2,4,8,9,11	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,7,17	2,4,8,9,11,15,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,7,16,18	2,4,8,9,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,7,14	2,4,8,9,11	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,7,14,16,17,18	2,4,8,9,11,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,7,14,18	2,4,8,9,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,7,14,16,17	2,4,8,9,11,15,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,7,17	2,4,8,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,7,16,18	2,4,8,9,11,13,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,7,17,18	2,4,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,7,16	2,4,8,9,11,13,15	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,7,14,18	2,4,8,9,11,13,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,7,14,16,17	2,4,8,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7,14	2,4,8,9,11,13,15	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,7,14,16,17,18	2,4,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,7,12	2,4,8,9,11	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,7,12,16,17,18	2,4,8,9,11,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,7,12,18	2,4,8,9,11,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,7,12,16,17	2,4,8,9,11,15,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,7,12,14,17,18	2,4,8,9,11,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,7,12,14,16	2,4,8,9,11	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,7,12,14,17	2,4,8,9,11,15,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,7,12,14,16,18	2,4,8,9,11,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7,12,18	2,4,8,9,11,13,18	2^{-34}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,7,12,16,17	2,4,8,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7,12	2,4,8,9,11,13,15	2^{-34}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,7,12,16,17,18	2,4,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,7,12,14,17	2,4,8,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,7,12,14,16,18	2,4,8,9,11,13,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,7,12,14,17,18	2,4,8,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,7,12,14,16	2,4,8,9,11,13,15	2^{-23}

Table 0.2015 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,10,18	2,4,8,9,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,7,10,16,17	2,4,8,9,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,10	2,4,8,9,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,7,10,16,17,18	2,4,8,9,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,7,10,14,17	2,4,8,9,17	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,10,14,16,18	2,4,8,9,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,7,10,14,17,18	2,4,8,9,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,10,14,16	2,4,8,9,15	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,7,10	2,4,8,9,13	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,7,10,16,17,18	2,4,8,9,13,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,7,10,18	2,4,8,9,13,15,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,7,10,16,17	2,4,8,9,13,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,7,10,14,17,18	2,4,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,7,10,14,16	2,4,8,9,13	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,7,10,14,17	2,4,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,7,10,14,16,18	2,4,8,9,13,15,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,7,10,12,17	2,4,8,9,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,7,10,12,16,18	2,4,8,9,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,7,10,12,17,18	2,4,8,9,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,7,10,12,16	2,4,8,9,15	$2^{-6.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,7,10,12,14,18	2,4,8,9,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,12,14,16,17	2,4,8,9,17	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,7,10,12,14	2,4,8,9,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,12,14,16,17,18	2,4,8,9,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,7,10,12,17,18	2,4,8,9,13,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,7,10,12,16	2,4,8,9,13	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,7,10,12,17	2,4,8,9,13,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,7,10,12,16,18	2,4,8,9,13,15,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,7,10,12,14	2,4,8,9,13	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,12,14,16,17,18	2,4,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,7,10,12,14,18	2,4,8,9,13,15,18	2^{-12}
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,12,14,16,17	2,4,8,9,13,15,17	$2^{-17.5}$

Table 0.2016 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		P
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,7,10	2,4,8,9,11	2 ⁻
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,7,10,16,17,18	2,4,8,9,11,17,18	2 ⁻
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,7,10,18	2,4,8,9,11,15,18	2 ⁻
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,7,10,16,17	2,4,8,9,11,15,17	2 ⁻
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,7,10,14,17,18	2,4,8,9,11,17,18	2 ⁻
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,7,10,14,16	2,4,8,9,11	2 ⁻
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,7,10,14,17	2,4,8,9,11,15,17	2 ⁻
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,7,10,14,16,18	2,4,8,9,11,15,18	2 ⁻
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,7,10,18	2,4,8,9,11,13,18	2 ⁻
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,10,16,17	2,4,8,9,11,13,17	2 ⁻
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,7,10	2,4,8,9,11,13,15	2 ⁻
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,10,16,17,18	2,4,8,9,11,13,15,17,18	2 ⁻
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,7,10,14,17	2,4,8,9,11,13,17	2 ⁻
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,7,10,14,16,18	2,4,8,9,11,13,18	2 ⁻
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,7,10,14,17,18	2,4,8,9,11,13,15,17,18	2 ⁻
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,7,10,14,16	2,4,8,9,11,13,15	2 ⁻
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,7,10,12,17,18	2,4,8,9,11,17,18	2 ⁻
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,7,10,12,16	2,4,8,9,11	2 ⁻
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,7,10,12,17	2,4,8,9,11,15,17	2 ⁻
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,7,10,12,16,18	2,4,8,9,11,15,18	2 ⁻
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,7,10,12,14	2,4,8,9,11	2 ⁻
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,7,10,12,14,16,17,18	2,4,8,9,11,17,18	2 ⁻
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,7,10,12,14,18	2,4,8,9,11,15,18	2 ⁻
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,7,10,12,14,16,17	2,4,8,9,11,15,17	2 ⁻
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,7,10,12,17	2,4,8,9,11,13,17	2 ⁻
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,7,10,12,16,18	2,4,8,9,11,13,18	2 ⁻
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,7,10,12,17,18	2,4,8,9,11,13,15,17,18	2 ⁻
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,7,10,12,16	2,4,8,9,11,13,15	2 ⁻
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,7,10,12,14,18	2,4,8,9,11,13,18	2 ⁻
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,7,10,12,14,16,17	2,4,8,9,11,13,17	2 ⁻
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,7,10,12,14	2,4,8,9,11,13,15	2 ⁻
$(1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,7,10,12,14,16,17,18	2,4,8,9,11,13,15,17,18	2 ⁻

Table 0.2017 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,17	2,4,6,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,16,18	2,4,6,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,17,18	2,4,6,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,16	2,4,6,15	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,14,18	2,4,6,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,14,16,17	2,4,6,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,14	2,4,6,15	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,14,16,17,18	2,4,6,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,17,18	2,4,6,13,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,16	2,4,6,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,17	2,4,6,13,15,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,16,18	2,4,6,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,14	2,4,6,13	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,14,16,17,18	2,4,6,13,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,14,18	2,4,6,13,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,14,16,17	2,4,6,13,15,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,12,18	2,4,6,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,12,16,17	2,4,6,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,12	2,4,6,15	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,12,16,17,18	2,4,6,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,12,14,17	2,4,6,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,12,14,16,18	2,4,6,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,12,14,17,18	2,4,6,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,12,14,16	2,4,6,15	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,12	2,4,6,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,12,16,17,18	2,4,6,13,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,12,18	2,4,6,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,12,16,17	2,4,6,13,15,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,12,14,17,18	2,4,6,13,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,12,14,16	2,4,6,13	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,12,14,17	2,4,6,13,15,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,12,14,16,18	2,4,6,13,15,18	$2^{-28.5}$

Table 0.2018 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,17,18	2,4,6,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,16	2,4,6,11	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,17	2,4,6,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,16,18	2,4,6,11,15,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,14	2,4,6,11	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,14,16,17,18	2,4,6,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,14,18	2,4,6,11,15,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,14,16,17	2,4,6,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,17	2,4,6,11,13,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,16,18	2,4,6,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,17,18	2,4,6,11,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,16	2,4,6,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,14,18	2,4,6,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,14,16,17	2,4,6,11,13,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,14	2,4,6,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,14,16,17,18	2,4,6,11,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,12	2,4,6,11	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,12,16,17,18	2,4,6,11,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,12,18	2,4,6,11,15,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,12,16,17	2,4,6,11,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,12,14,17,18	2,4,6,11,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,12,14,16	2,4,6,11	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,12,14,17	2,4,6,11,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,12,14,16,18	2,4,6,11,15,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,12,18	2,4,6,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,12,16,17	2,4,6,11,13,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,12	2,4,6,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,12,16,17,18	2,4,6,11,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,12,14,17	2,4,6,11,13,17	2^{-1}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,12,14,16,18	2,4,6,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,12,14,17,18	2,4,6,11,13,15,17,18	2^{-1}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,12,14,16	2,4,6,11,13,15	$2^{-17.5}$

Table 0.2019 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,10,18	2,4,6,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,10,16,17	2,4,6,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,10	2,4,6,15	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,10,16,17,18	2,4,6,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,10,14,17	2,4,6,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,10,14,16,18	2,4,6,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,10,14,17,18	2,4,6,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,10,14,16	2,4,6,15	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,10	2,4,6,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,10,16,17,18	2,4,6,13,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,10,18	2,4,6,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,10,16,17	2,4,6,13,15,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,10,14,17,18	2,4,6,13,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,10,14,16	2,4,6,13	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,10,14,17	2,4,6,13,15,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,10,14,16,18	2,4,6,13,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,10,12,17	2,4,6,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,10,12,16,18	2,4,6,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,10,12,17,18	2,4,6,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,10,12,16	2,4,6,15	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,10,12,14,18	2,4,6,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,10,12,14,16,17	2,4,6,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,10,12,14	2,4,6,15	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,10,12,14,16,17,18	2,4,6,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,10,12,17,18	2,4,6,13,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,10,12,16	2,4,6,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,10,12,17	2,4,6,13,15,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,10,12,16,18	2,4,6,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,10,12,14	2,4,6,13	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,10,12,14,16,17,18	2,4,6,13,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,10,12,14,18	2,4,6,13,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,10,12,14,16,17	2,4,6,13,15,17	2^{-23}

Table 0.2020 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,10	2,4,6,11	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,10,16,17,18	2,4,6,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,10,18	2,4,6,11,15,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,10,16,17	2,4,6,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,10,14,17,18	2,4,6,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,10,14,16	2,4,6,11	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,10,14,17	2,4,6,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,10,14,16,18	2,4,6,11,15,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,10,18	2,4,6,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,10,16,17	2,4,6,11,13,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,10	2,4,6,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,10,16,17,18	2,4,6,11,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,10,14,17	2,4,6,11,13,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,10,14,16,18	2,4,6,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,10,14,17,18	2,4,6,11,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,10,14,16	2,4,6,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,10,12,17,18	2,4,6,11,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,10,12,16	2,4,6,11	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,10,12,17	2,4,6,11,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,10,12,16,18	2,4,6,11,15,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,10,12,14	2,4,6,11	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,10,12,14,16,17,18	2,4,6,11,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,10,12,14,18	2,4,6,11,15,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,10,12,14,16,17	2,4,6,11,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,10,12,17	2,4,6,11,13,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,10,12,16,18	2,4,6,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,10,12,17,18	2,4,6,11,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,10,12,16	2,4,6,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,10,12,14,18	2,4,6,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,10,12,14,16,17	2,4,6,11,13,17	2^{-34}
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,10,12,14	2,4,6,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,10,12,14,16,17,18	2,4,6,11,13,15,17,18	2^{-34}

Table 0.2021 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,17,18	2,4,6,9,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,16	2,4,6,9	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,17	2,4,6,9,15,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,16,18	2,4,6,9,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,14	2,4,6,9	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,14,16,17,18	2,4,6,9,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,14,18	2,4,6,9,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,14,16,17	2,4,6,9,15,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,17	2,4,6,9,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,16,18	2,4,6,9,13,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,17,18	2,4,6,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,16	2,4,6,9,13,15	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,14,18	2,4,6,9,13,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,14,16,17	2,4,6,9,13,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,14	2,4,6,9,13,15	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,14,16,17,18	2,4,6,9,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,12	2,4,6,9	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,12,16,17,18	2,4,6,9,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,12,18	2,4,6,9,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,12,16,17	2,4,6,9,15,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,12,14,17,18	2,4,6,9,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,12,14,16	2,4,6,9	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,12,14,17	2,4,6,9,15,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,12,14,16,18	2,4,6,9,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,12,18	2,4,6,9,13,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,12,16,17	2,4,6,9,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,12	2,4,6,9,13,15	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,12,16,17,18	2,4,6,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,12,14,17	2,4,6,9,13,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,12,14,16,18	2,4,6,9,13,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,12,14,17,18	2,4,6,9,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,12,14,16	2,4,6,9,13,15	2^{-23}

Table 0.2022 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,17	2,4,6,9,11,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,16,18	2,4,6,9,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,17,18	2,4,6,9,11,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,16	2,4,6,9,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,14,18	2,4,6,9,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,14,16,17	2,4,6,9,11,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,14	2,4,6,9,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,14,16,17,18	2,4,6,9,11,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,17,18	2,4,6,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,16	2,4,6,9,11,13	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,17	2,4,6,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,16,18	2,4,6,9,11,13,15,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,14	2,4,6,9,11,13	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,14,16,17,18	2,4,6,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,14,18	2,4,6,9,11,13,15,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,14,16,17	2,4,6,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,12,18	2,4,6,9,11,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,12,16,17	2,4,6,9,11,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,12	2,4,6,9,11,15	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,12,16,17,18	2,4,6,9,11,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,12,14,17	2,4,6,9,11,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,12,14,16,18	2,4,6,9,11,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,12,14,17,18	2,4,6,9,11,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,12,14,16	2,4,6,9,11,15	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,12	2,4,6,9,11,13	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,12,16,17,18	2,4,6,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,12,18	2,4,6,9,11,13,15,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,12,16,17	2,4,6,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,12,14,17,18	2,4,6,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,12,14,16	2,4,6,9,11,13	2^{-34}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,12,14,17	2,4,6,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,12,14,16,18	2,4,6,9,11,13,15,18	2^{-34}

Table 0.2023 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,10	2,4,6,9	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,10,16,17,18	2,4,6,9,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,10,18	2,4,6,9,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,10,16,17	2,4,6,9,15,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,10,14,17,18	2,4,6,9,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,10,14,16	2,4,6,9	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,10,14,17	2,4,6,9,15,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,10,14,16,18	2,4,6,9,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,10,18	2,4,6,9,13,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,10,16,17	2,4,6,9,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,10	2,4,6,9,13,15	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,10,16,17,18	2,4,6,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,10,14,17	2,4,6,9,13,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,10,14,16,18	2,4,6,9,13,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,10,14,17,18	2,4,6,9,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,10,14,16	2,4,6,9,13,15	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,10,12,17,18	2,4,6,9,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,10,12,16	2,4,6,9	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,10,12,17	2,4,6,9,15,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,10,12,16,18	2,4,6,9,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,10,12,14	2,4,6,9	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,10,12,14,16,17,18	2,4,6,9,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,10,12,14,18	2,4,6,9,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,10,12,14,16,17	2,4,6,9,15,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,10,12,17	2,4,6,9,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,10,12,16,18	2,4,6,9,13,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,10,12,17,18	2,4,6,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,10,12,16	2,4,6,9,13,15	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,10,12,14,18	2,4,6,9,13,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,10,12,14,16,17	2,4,6,9,13,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,10,12,14	2,4,6,9,13,15	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,10,12,14,16,17,18	2,4,6,9,13,15,17,18	$2^{-28.5}$

Table 0.2024 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,10,18	2,4,6,9,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,10,16,17	2,4,6,9,11,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,10	2,4,6,9,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,10,16,17,18	2,4,6,9,11,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,10,14,17	2,4,6,9,11,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,10,14,16,18	2,4,6,9,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,10,14,17,18	2,4,6,9,11,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,10,14,16	2,4,6,9,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,10	2,4,6,9,11,13	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,10,16,17,18	2,4,6,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,10,18	2,4,6,9,11,13,15,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,10,16,17	2,4,6,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,10,14,17,18	2,4,6,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,10,14,16	2,4,6,9,11,13	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,10,14,17	2,4,6,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,10,14,16,18	2,4,6,9,11,13,15,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,10,12,17	2,4,6,9,11,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,10,12,16,18	2,4,6,9,11,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,10,12,17,18	2,4,6,9,11,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,10,12,16	2,4,6,9,11,15	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,10,12,14,18	2,4,6,9,11,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,10,12,14,16,17	2,4,6,9,11,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,10,12,14	2,4,6,9,11,15	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,10,12,14,16,17,18	2,4,6,9,11,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,10,12,17,18	2,4,6,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,10,12,16	2,4,6,9,11,13	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,10,12,17	2,4,6,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,10,12,16,18	2,4,6,9,11,13,15,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,10,12,14	2,4,6,9,11,13	2^{-1}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,10,12,14,16,17,18	2,4,6,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,10,12,14,18	2,4,6,9,11,13,15,18	2^{-1}
$(1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,10,12,14,16,17	2,4,6,9,11,13,15,17	$2^{-17.5}$

Table 0.2025 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,18	2,4,6,8,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,16,17	2,4,6,8,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,5	2,4,6,8,15	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,16,17,18	2,4,6,8,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,14,17	2,4,6,8,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,14,16,18	2,4,6,8,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,14,17,18	2,4,6,8,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,14,16	2,4,6,8,15	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,5	2,4,6,8,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,16,17,18	2,4,6,8,13,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,18	2,4,6,8,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,16,17	2,4,6,8,13,15,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,14,17,18	2,4,6,8,13,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,14,16	2,4,6,8,13	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,14,17	2,4,6,8,13,15,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,14,16,18	2,4,6,8,13,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,12,17	2,4,6,8,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,12,16,18	2,4,6,8,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,12,17,18	2,4,6,8,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,12,16	2,4,6,8,15	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,12,14,18	2,4,6,8,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,12,14,16,17	2,4,6,8,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,12,14	2,4,6,8,15	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,12,14,16,17,18	2,4,6,8,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,12,17,18	2,4,6,8,13,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,12,16	2,4,6,8,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,12,17	2,4,6,8,13,15,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,12,16,18	2,4,6,8,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,12,14	2,4,6,8,13	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,12,14,16,17,18	2,4,6,8,13,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,12,14,18	2,4,6,8,13,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,12,14,16,17	2,4,6,8,13,15,17	2^{-12}

Table 0.2026 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,5	2,4,6,8,11	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,16,17,18	2,4,6,8,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,18	2,4,6,8,11,15,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,16,17	2,4,6,8,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,14,17,18	2,4,6,8,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,14,16	2,4,6,8,11	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,14,17	2,4,6,8,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,14,16,18	2,4,6,8,11,15,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,18	2,4,6,8,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,16,17	2,4,6,8,11,13,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5	2,4,6,8,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,16,17,18	2,4,6,8,11,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,14,17	2,4,6,8,11,13,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,14,16,18	2,4,6,8,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,14,17,18	2,4,6,8,11,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,14,16	2,4,6,8,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,12,17,18	2,4,6,8,11,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,12,16	2,4,6,8,11	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,12,17	2,4,6,8,11,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,12,16,18	2,4,6,8,11,15,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,12,14	2,4,6,8,11	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,12,14,16,17,18	2,4,6,8,11,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,12,14,18	2,4,6,8,11,15,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,12,14,16,17	2,4,6,8,11,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,12,17	2,4,6,8,11,13,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,12,16,18	2,4,6,8,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,12,17,18	2,4,6,8,11,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,12,16	2,4,6,8,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,12,14,18	2,4,6,8,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,12,14,16,17	2,4,6,8,11,13,17	2^{-1}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,12,14	2,4,6,8,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,12,14,16,17,18	2,4,6,8,11,13,15,17,18	2^{-1}

Table 0.2027 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,10,17	2,4,6,8,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,10,16,18	2,4,6,8,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,10,17,18	2,4,6,8,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,10,16	2,4,6,8,15	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,10,14,18	2,4,6,8,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,10,14,16,17	2,4,6,8,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,10,14	2,4,6,8,15	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,10,14,16,17,18	2,4,6,8,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,10,17,18	2,4,6,8,13,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,10,16	2,4,6,8,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,10,17	2,4,6,8,13,15,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,10,16,18	2,4,6,8,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,10,14	2,4,6,8,13	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,10,14,16,17,18	2,4,6,8,13,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,10,14,18	2,4,6,8,13,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,10,14,16,17	2,4,6,8,13,15,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,10,12,18	2,4,6,8,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,10,12,16,17	2,4,6,8,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,10,12	2,4,6,8,15	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,10,12,16,17,18	2,4,6,8,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,10,12,14,17	2,4,6,8,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,10,12,14,16,18	2,4,6,8,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,10,12,14,17,18	2,4,6,8,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,10,12,14,16	2,4,6,8,15	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,10,12	2,4,6,8,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,10,12,16,17,18	2,4,6,8,13,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,10,12,18	2,4,6,8,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,10,12,16,17	2,4,6,8,13,15,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,10,12,14,17,18	2,4,6,8,13,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,10,12,14,16	2,4,6,8,13	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,10,12,14,17	2,4,6,8,13,15,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,10,12,14,16,18	2,4,6,8,13,15,18	$2^{-6.5}$

Table 0.2028 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,10,17,18	2,4,6,8,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,10,16	2,4,6,8,11	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,10,17	2,4,6,8,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,10,16,18	2,4,6,8,11,15,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,10,14	2,4,6,8,11	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,10,14,16,17,18	2,4,6,8,11,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,10,14,18	2,4,6,8,11,15,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,10,14,16,17	2,4,6,8,11,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,10,17	2,4,6,8,11,13,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,10,16,18	2,4,6,8,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,10,17,18	2,4,6,8,11,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,10,16	2,4,6,8,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,10,14,18	2,4,6,8,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,10,14,16,17	2,4,6,8,11,13,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,10,14	2,4,6,8,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,10,14,16,17,18	2,4,6,8,11,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,10,12	2,4,6,8,11	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,10,12,16,17,18	2,4,6,8,11,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,10,12,18	2,4,6,8,11,15,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,10,12,16,17	2,4,6,8,11,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,10,12,14,17,18	2,4,6,8,11,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,10,12,14,16	2,4,6,8,11	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,10,12,14,17	2,4,6,8,11,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,10,12,14,16,18	2,4,6,8,11,15,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,10,12,18	2,4,6,8,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,10,12,16,17	2,4,6,8,11,13,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,10,12	2,4,6,8,11,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,10,12,16,17,18	2,4,6,8,11,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,10,12,14,17	2,4,6,8,11,13,17	2^{-34}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,10,12,14,16,18	2,4,6,8,11,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,10,12,14,17,18	2,4,6,8,11,13,15,17,18	2^{-34}
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,10,12,14,16	2,4,6,8,11,13,15	$2^{-17.5}$

Table 0.2029 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,5	2,4,6,8,9	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,16,17,18	2,4,6,8,9,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,18	2,4,6,8,9,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,16,17	2,4,6,8,9,15,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,14,17,18	2,4,6,8,9,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,14,16	2,4,6,8,9	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,14,17	2,4,6,8,9,15,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,14,16,18	2,4,6,8,9,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,18	2,4,6,8,9,13,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,16,17	2,4,6,8,9,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,5	2,4,6,8,9,13,15	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,16,17,18	2,4,6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,14,17	2,4,6,8,9,13,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,14,16,18	2,4,6,8,9,13,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,14,17,18	2,4,6,8,9,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,14,16	2,4,6,8,9,13,15	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,12,17,18	2,4,6,8,9,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,12,16	2,4,6,8,9	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,12,17	2,4,6,8,9,15,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,12,16,18	2,4,6,8,9,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,12,14	2,4,6,8,9	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,12,14,16,17,18	2,4,6,8,9,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,12,14,18	2,4,6,8,9,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,12,14,16,17	2,4,6,8,9,15,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,12,17	2,4,6,8,9,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,12,16,18	2,4,6,8,9,13,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,12,17,18	2,4,6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,12,16	2,4,6,8,9,13,15	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,12,14,18	2,4,6,8,9,13,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,12,14,16,17	2,4,6,8,9,13,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,12,14	2,4,6,8,9,13,15	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,12,14,16,17,18	2,4,6,8,9,13,15,17,18	$2^{-6.5}$

Table 0.2030 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,18	2,4,6,8,9,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,16,17	2,4,6,8,9,11,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,5	2,4,6,8,9,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,16,17,18	2,4,6,8,9,11,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,14,17	2,4,6,8,9,11,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,14,16,18	2,4,6,8,9,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,14,17,18	2,4,6,8,9,11,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,14,16	2,4,6,8,9,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,5	2,4,6,8,9,11,13	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,16,17,18	2,4,6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,18	2,4,6,8,9,11,13,15,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,16,17	2,4,6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,14,17,18	2,4,6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,14,16	2,4,6,8,9,11,13	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,14,17	2,4,6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,14,16,18	2,4,6,8,9,11,13,15,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,12,17	2,4,6,8,9,11,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,12,16,18	2,4,6,8,9,11,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,12,17,18	2,4,6,8,9,11,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,12,16	2,4,6,8,9,11,15	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,12,14,18	2,4,6,8,9,11,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,12,14,16,17	2,4,6,8,9,11,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,12,14	2,4,6,8,9,11,15	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,12,14,16,17,18	2,4,6,8,9,11,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,12,17,18	2,4,6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,12,16	2,4,6,8,9,11,13	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,12,17	2,4,6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,12,16,18	2,4,6,8,9,11,13,15,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,12,14	2,4,6,8,9,11,13	2^{-34}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,12,14,16,17,18	2,4,6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,12,14,18	2,4,6,8,9,11,13,15,18	2^{-34}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,12,14,16,17	2,4,6,8,9,11,13,15,17	$2^{-17.5}$

Table 0.2031 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,10,17,18	2,4,6,8,9,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,10,16	2,4,6,8,9	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,10,17	2,4,6,8,9,15,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,10,16,18	2,4,6,8,9,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,10,14	2,4,6,8,9	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,10,14,16,17,18	2,4,6,8,9,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,10,14,18	2,4,6,8,9,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,10,14,16,17	2,4,6,8,9,15,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,10,17	2,4,6,8,9,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,10,16,18	2,4,6,8,9,13,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,10,17,18	2,4,6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,10,16	2,4,6,8,9,13,15	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,10,14,18	2,4,6,8,9,13,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,10,14,16,17	2,4,6,8,9,13,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,10,14	2,4,6,8,9,13,15	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,10,14,16,17,18	2,4,6,8,9,13,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,10,12	2,4,6,8,9	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,10,12,16,17,18	2,4,6,8,9,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,10,12,18	2,4,6,8,9,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,10,12,16,17	2,4,6,8,9,15,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,10,12,14,17,18	2,4,6,8,9,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,10,12,14,16	2,4,6,8,9	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,10,12,14,17	2,4,6,8,9,15,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,10,12,14,16,18	2,4,6,8,9,15,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,10,12,18	2,4,6,8,9,13,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,10,12,16,17	2,4,6,8,9,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,10,12	2,4,6,8,9,13,15	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,10,12,16,17,18	2,4,6,8,9,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,10,12,14,17	2,4,6,8,9,13,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,10,12,14,16,18	2,4,6,8,9,13,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,10,12,14,17,18	2,4,6,8,9,13,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,10,12,14,16	2,4,6,8,9,13,15	2^{-12}

Table 0.2032 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,10,17	2,4,6,8,9,11,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,10,16,18	2,4,6,8,9,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,10,17,18	2,4,6,8,9,11,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,10,16	2,4,6,8,9,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,10,14,18	2,4,6,8,9,11,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,10,14,16,17	2,4,6,8,9,11,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,10,14	2,4,6,8,9,11,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,10,14,16,17,18	2,4,6,8,9,11,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,10,17,18	2,4,6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,10,16	2,4,6,8,9,11,13	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,10,17	2,4,6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,10,16,18	2,4,6,8,9,11,13,15,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,10,14	2,4,6,8,9,11,13	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,10,14,16,17,18	2,4,6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,10,14,18	2,4,6,8,9,11,13,15,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,10,14,16,17	2,4,6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,10,12,18	2,4,6,8,9,11,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,10,12,16,17	2,4,6,8,9,11,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,10,12	2,4,6,8,9,11,15	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,10,12,16,17,18	2,4,6,8,9,11,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,10,12,14,17	2,4,6,8,9,11,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,10,12,14,16,18	2,4,6,8,9,11,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,10,12,14,17,18	2,4,6,8,9,11,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,10,12,14,16	2,4,6,8,9,11,15	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,10,12	2,4,6,8,9,11,13	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,10,12,16,17,18	2,4,6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,10,12,18	2,4,6,8,9,11,13,15,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,10,12,16,17	2,4,6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,10,12,14,17,18	2,4,6,8,9,11,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,10,12,14,16	2,4,6,8,9,11,13	2^{-1}
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,10,12,14,17	2,4,6,8,9,11,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,10,12,14,16,18	2,4,6,8,9,11,13,15,18	2^{-1}

Table 0.2033 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,7,17,18	2,4,6,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,7,16	2,4,6	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,7,17	2,4,6,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,7,16,18	2,4,6,15,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,7,14	2,4,6	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,7,14,16,17,18	2,4,6,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,7,14,18	2,4,6,15,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,7,14,16,17	2,4,6,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,7,17	2,4,6,13,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,7,16,18	2,4,6,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,7,17,18	2,4,6,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,7,16	2,4,6,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,7,14,18	2,4,6,13,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,7,14,16,17	2,4,6,13,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,7,14	2,4,6,13,15	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,7,14,16,17,18	2,4,6,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,7,12	2,4,6	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,7,12,16,17,18	2,4,6,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,7,12,18	2,4,6,15,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,7,12,16,17	2,4,6,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,7,12,14,17,18	2,4,6,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,7,12,14,16	2,4,6	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,7,12,14,17	2,4,6,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,7,12,14,16,18	2,4,6,15,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,7,12,18	2,4,6,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,7,12,16,17	2,4,6,13,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,7,12	2,4,6,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,7,12,16,17,18	2,4,6,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,7,12,14,17	2,4,6,13,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,7,12,14,16,18	2,4,6,13,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,7,12,14,17,18	2,4,6,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,7,12,14,16	2,4,6,13,15	$2^{-28.5}$

Table 0.2034 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,7,17	2,4,6,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,7,16,18	2,4,6,11,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,7,17,18	2,4,6,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,7,16	2,4,6,11,15	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,7,14,18	2,4,6,11,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,7,14,16,17	2,4,6,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,7,14	2,4,6,11,15	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,7,14,16,17,18	2,4,6,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,7,17,18	2,4,6,11,13,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,7,16	2,4,6,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,7,17	2,4,6,11,13,15,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,7,16,18	2,4,6,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,7,14	2,4,6,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7,14,16,17,18	2,4,6,11,13,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,7,14,18	2,4,6,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7,14,16,17	2,4,6,11,13,15,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,7,12,18	2,4,6,11,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,7,12,16,17	2,4,6,11,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,7,12	2,4,6,11,15	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,7,12,16,17,18	2,4,6,11,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,7,12,14,17	2,4,6,11,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,7,12,14,16,18	2,4,6,11,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,7,12,14,17,18	2,4,6,11,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,7,12,14,16	2,4,6,11,15	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,7,12	2,4,6,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,7,12,16,17,18	2,4,6,11,13,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,7,12,18	2,4,6,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,7,12,16,17	2,4,6,11,13,15,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,7,12,14,17,18	2,4,6,11,13,17,18	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,7,12,14,16	2,4,6,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,7,12,14,17	2,4,6,11,13,15,17	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,7,12,14,16,18	2,4,6,11,13,15,18	$2^{-17.5}$

Table 0.2035 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10	2,4,6	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,7,10,16,17,18	2,4,6,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,18	2,4,6,15,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,7,10,16,17	2,4,6,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,7,10,14,17,18	2,4,6,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,7,10,14,16	2,4,6	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,7,10,14,17	2,4,6,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,7,10,14,16,18	2,4,6,15,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10,18	2,4,6,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,7,10,16,17	2,4,6,13,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,7,10	2,4,6,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,7,10,16,17,18	2,4,6,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,7,10,14,17	2,4,6,13,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,7,10,14,16,18	2,4,6,13,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,7,10,14,17,18	2,4,6,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,7,10,14,16	2,4,6,13,15	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,10,12,17,18	2,4,6,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,7,10,12,16	2,4,6	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,10,12,17	2,4,6,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,7,10,12,16,18	2,4,6,15,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,7,10,12,14	2,4,6	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,10,12,14,16,17,18	2,4,6,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,7,10,12,14,18	2,4,6,15,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,10,12,14,16,17	2,4,6,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,7,10,12,17	2,4,6,13,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,7,10,12,16,18	2,4,6,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,7,10,12,17,18	2,4,6,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,7,10,12,16	2,4,6,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,7,10,12,14,18	2,4,6,13,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,7,10,12,14,16,17	2,4,6,13,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,7,10,12,14	2,4,6,13,15	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,7,10,12,14,16,17,18	2,4,6,13,15,17,18	2^{-23}

Table 0.2036 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,7,10,18	2,4,6,11,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,7,10,16,17	2,4,6,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,7,10	2,4,6,11,15	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,7,10,16,17,18	2,4,6,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,7,10,14,17	2,4,6,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,7,10,14,16,18	2,4,6,11,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,7,10,14,17,18	2,4,6,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,7,10,14,16	2,4,6,11,15	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,7,10	2,4,6,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,7,10,16,17,18	2,4,6,11,13,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,7,10,18	2,4,6,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,7,10,16,17	2,4,6,11,13,15,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,7,10,14,17,18	2,4,6,11,13,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,7,10,14,16	2,4,6,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,7,10,14,17	2,4,6,11,13,15,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,7,10,14,16,18	2,4,6,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,7,10,12,17	2,4,6,11,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,7,10,12,16,18	2,4,6,11,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,7,10,12,17,18	2,4,6,11,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,7,10,12,16	2,4,6,11,15	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,7,10,12,14,18	2,4,6,11,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,7,10,12,14,16,17	2,4,6,11,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,7,10,12,14	2,4,6,11,15	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,7,10,12,14,16,17,18	2,4,6,11,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,7,10,12,17,18	2,4,6,11,13,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,7,10,12,16	2,4,6,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,7,10,12,17	2,4,6,11,13,15,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,7,10,12,16,18	2,4,6,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,10,12,14	2,4,6,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,7,10,12,14,16,17,18	2,4,6,11,13,17,18	2^{-34}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,10,12,14,18	2,4,6,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,7,10,12,14,16,17	2,4,6,11,13,15,17	2^{-34}

Table 0.2037 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,7,17	2,4,6,9,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,7,16,18	2,4,6,9,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,7,17,18	2,4,6,9,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,7,16	2,4,6,9,15	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,7,14,18	2,4,6,9,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,7,14,16,17	2,4,6,9,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,7,14	2,4,6,9,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,7,14,16,17,18	2,4,6,9,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,7,17,18	2,4,6,9,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,7,16	2,4,6,9,13	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,7,17	2,4,6,9,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,7,16,18	2,4,6,9,13,15,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,7,14	2,4,6,9,13	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,7,14,16,17,18	2,4,6,9,13,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,7,14,18	2,4,6,9,13,15,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,7,14,16,17	2,4,6,9,13,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,7,12,18	2,4,6,9,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,7,12,16,17	2,4,6,9,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,7,12	2,4,6,9,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,7,12,16,17,18	2,4,6,9,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,7,12,14,17	2,4,6,9,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,7,12,14,16,18	2,4,6,9,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,7,12,14,17,18	2,4,6,9,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,7,12,14,16	2,4,6,9,15	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,7,12	2,4,6,9,13	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,7,12,16,17,18	2,4,6,9,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,7,12,18	2,4,6,9,13,15,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,7,12,16,17	2,4,6,9,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,7,12,14,17,18	2,4,6,9,13,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,7,12,14,16	2,4,6,9,13	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,7,12,14,17	2,4,6,9,13,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,7,12,14,16,18	2,4,6,9,13,15,18	2^{-23}

Table 0.2038 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,7,17,18	2,4,6,9,11,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,7,16	2,4,6,9,11	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,7,17	2,4,6,9,11,15,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,7,16,18	2,4,6,9,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,7,14	2,4,6,9,11	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,7,14,16,17,18	2,4,6,9,11,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,7,14,18	2,4,6,9,11,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7,14,16,17	2,4,6,9,11,15,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,7,17	2,4,6,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,7,16,18	2,4,6,9,11,13,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,7,17,18	2,4,6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,7,16	2,4,6,9,11,13,15	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,7,14,18	2,4,6,9,11,13,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,7,14,16,17	2,4,6,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,7,14	2,4,6,9,11,13,15	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,7,14,16,17,18	2,4,6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,7,12	2,4,6,9,11	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,7,12,16,17,18	2,4,6,9,11,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,7,12,18	2,4,6,9,11,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,7,12,16,17	2,4,6,9,11,15,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,7,12,14,17,18	2,4,6,9,11,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,7,12,14,16	2,4,6,9,11	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,7,12,14,17	2,4,6,9,11,15,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,7,12,14,16,18	2,4,6,9,11,15,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,7,12,18	2,4,6,9,11,13,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7,12,16,17	2,4,6,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,7,12	2,4,6,9,11,13,15	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,7,12,16,17,18	2,4,6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,7,12,14,17	2,4,6,9,11,13,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,7,12,14,16,18	2,4,6,9,11,13,18	2^{-34}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,7,12,14,17,18	2,4,6,9,11,13,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,7,12,14,16	2,4,6,9,11,13,15	2^{-34}

Table 0.2039 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,7,10,18	2,4,6,9,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,7,10,16,17	2,4,6,9,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,7,10	2,4,6,9,15	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,7,10,16,17,18	2,4,6,9,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,7,10,14,17	2,4,6,9,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,7,10,14,16,18	2,4,6,9,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,7,10,14,17,18	2,4,6,9,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,7,10,14,16	2,4,6,9,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,7,10	2,4,6,9,13	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,7,10,16,17,18	2,4,6,9,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,7,10,18	2,4,6,9,13,15,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,7,10,16,17	2,4,6,9,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,7,10,14,17,18	2,4,6,9,13,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,7,10,14,16	2,4,6,9,13	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,7,10,14,17	2,4,6,9,13,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,7,10,14,16,18	2,4,6,9,13,15,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,7,10,12,17	2,4,6,9,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,7,10,12,16,18	2,4,6,9,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,7,10,12,17,18	2,4,6,9,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,7,10,12,16	2,4,6,9,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,7,10,12,14,18	2,4,6,9,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,7,10,12,14,16,17	2,4,6,9,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,7,10,12,14	2,4,6,9,15	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,7,10,12,14,16,17,18	2,4,6,9,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,7,10,12,17,18	2,4,6,9,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,7,10,12,16	2,4,6,9,13	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,7,10,12,17	2,4,6,9,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,7,10,12,16,18	2,4,6,9,13,15,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,7,10,12,14	2,4,6,9,13	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,7,10,12,14,16,17,18	2,4,6,9,13,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,7,10,12,14,18	2,4,6,9,13,15,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,7,10,12,14,16,17	2,4,6,9,13,15,17	$2^{-28.5}$

Table 0.2040 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		P
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,7,10	2,4,6,9,11	2 ⁻
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,7,10,16,17,18	2,4,6,9,11,17,18	2 ⁻
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,7,10,18	2,4,6,9,11,15,18	2 ⁻
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,7,10,16,17	2,4,6,9,11,15,17	2 ⁻
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,7,10,14,17,18	2,4,6,9,11,17,18	2 ⁻
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,7,10,14,16	2,4,6,9,11	2 ⁻
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,7,10,14,17	2,4,6,9,11,15,17	2 ⁻
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,7,10,14,16,18	2,4,6,9,11,15,18	2 ⁻
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,7,10,18	2,4,6,9,11,13,18	2 ⁻
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,7,10,16,17	2,4,6,9,11,13,17	2 ⁻
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,7,10	2,4,6,9,11,13,15	2 ⁻
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,7,10,16,17,18	2,4,6,9,11,13,15,17,18	2 ⁻
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,7,10,14,17	2,4,6,9,11,13,17	2 ⁻
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,7,10,14,16,18	2,4,6,9,11,13,18	2 ⁻
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,7,10,14,17,18	2,4,6,9,11,13,15,17,18	2 ⁻
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1)$	1,3,5,7,10,14,16	2,4,6,9,11,13,15	2 ⁻
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,7,10,12,17,18	2,4,6,9,11,17,18	2 ⁻
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,7,10,12,16	2,4,6,9,11	2 ⁻
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,7,10,12,17	2,4,6,9,11,15,17	2 ⁻
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,7,10,12,16,18	2,4,6,9,11,15,18	2 ⁻
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,7,10,12,14	2,4,6,9,11	2 ⁻
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,7,10,12,14,16,17,18	2,4,6,9,11,17,18	2 ⁻
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,7,10,12,14,18	2,4,6,9,11,15,18	2 ⁻
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,7,10,12,14,16,17	2,4,6,9,11,15,17	2 ⁻
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,7,10,12,17	2,4,6,9,11,13,17	2 ⁻
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,7,10,12,16,18	2,4,6,9,11,13,18	2 ⁻
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,7,10,12,17,18	2,4,6,9,11,13,15,17,18	2 ⁻
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,7,10,12,16	2,4,6,9,11,13,15	2 ⁻
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,7,10,12,14,18	2,4,6,9,11,13,18	2 ⁻
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,7,10,12,14,16,17	2,4,6,9,11,13,17	2 ⁻
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,7,10,12,14	2,4,6,9,11,13,15	2 ⁻
$(1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,7,10,12,14,16,17,18	2,4,6,9,11,13,15,17,18	2 ⁻

Table 0.2041 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,7	2,4,6,8	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,7,16,17,18	2,4,6,8,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0)$	1,3,5,7,18	2,4,6,8,15,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0)$	1,3,5,7,16,17	2,4,6,8,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,7,14,17,18	2,4,6,8,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,7,14,16	2,4,6,8	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1)$	1,3,5,7,14,17	2,4,6,8,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1)$	1,3,5,7,14,16,18	2,4,6,8,15,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,7,18	2,4,6,8,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,7,16,17	2,4,6,8,13,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0)$	1,3,5,7	2,4,6,8,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0)$	1,3,5,7,16,17,18	2,4,6,8,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,7,14,17	2,4,6,8,13,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,7,14,16,18	2,4,6,8,13,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1)$	1,3,5,7,14,17,18	2,4,6,8,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1)$	1,3,5,7,14,16	2,4,6,8,13,15	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,7,12,17,18	2,4,6,8,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,7,12,16	2,4,6,8	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1)$	1,3,5,7,12,17	2,4,6,8,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1)$	1,3,5,7,12,16,18	2,4,6,8,15,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,7,12,14	2,4,6,8	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,7,12,14,16,17,18	2,4,6,8,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0)$	1,3,5,7,12,14,18	2,4,6,8,15,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$	1,3,5,7,12,14,16,17	2,4,6,8,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,7,12,17	2,4,6,8,13,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,7,12,16,18	2,4,6,8,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1)$	1,3,5,7,12,17,18	2,4,6,8,13,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1)$	1,3,5,7,12,16	2,4,6,8,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,7,12,14,18	2,4,6,8,13,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,7,12,14,16,17	2,4,6,8,13,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0)$	1,3,5,7,12,14	2,4,6,8,13,15	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0)$	1,3,5,7,12,14,16,17,18	2,4,6,8,13,15,17,18	2^{-12}

Table 0.2042 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,7,18	2,4,6,8,11,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,7,16,17	2,4,6,8,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0)$	1,3,5,7	2,4,6,8,11,15	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0)$	1,3,5,7,16,17,18	2,4,6,8,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,7,14,17	2,4,6,8,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,7,14,16,18	2,4,6,8,11,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1)$	1,3,5,7,14,17,18	2,4,6,8,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1)$	1,3,5,7,14,16	2,4,6,8,11,15	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,7	2,4,6,8,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,7,16,17,18	2,4,6,8,11,13,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0)$	1,3,5,7,18	2,4,6,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0)$	1,3,5,7,16,17	2,4,6,8,11,13,15,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,7,14,17,18	2,4,6,8,11,13,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,7,14,16	2,4,6,8,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,7,14,17	2,4,6,8,11,13,15,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 1)$	1,3,5,7,14,16,18	2,4,6,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,7,12,17	2,4,6,8,11,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,7,12,16,18	2,4,6,8,11,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1)$	1,3,5,7,12,17,18	2,4,6,8,11,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1)$	1,3,5,7,12,16	2,4,6,8,11,15	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,7,12,14,18	2,4,6,8,11,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,7,12,14,16,17	2,4,6,8,11,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0)$	1,3,5,7,12,14	2,4,6,8,11,15	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0)$	1,3,5,7,12,14,16,17,18	2,4,6,8,11,15,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,7,12,17,18	2,4,6,8,11,13,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,7,12,16	2,4,6,8,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1)$	1,3,5,7,12,17	2,4,6,8,11,13,15,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1)$	1,3,5,7,12,16,18	2,4,6,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,7,12,14	2,4,6,8,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,7,12,14,16,17,18	2,4,6,8,11,13,17,18	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)$	1,3,5,7,12,14,18	2,4,6,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0)$	1,3,5,7,12,14,16,17	2,4,6,8,11,13,15,17	2^{-1}

Table 0.2043 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,7,10,17,18	2,4,6,8,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,7,10,16	2,4,6,8	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1)$	1,3,5,7,10,17	2,4,6,8,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1)$	1,3,5,7,10,16,18	2,4,6,8,15,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,14	2,4,6,8	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10,14,16,17,18	2,4,6,8,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,14,18	2,4,6,8,15,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10,14,16,17	2,4,6,8,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,7,10,17	2,4,6,8,13,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,7,10,16,18	2,4,6,8,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1)$	1,3,5,7,10,17,18	2,4,6,8,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1)$	1,3,5,7,10,16	2,4,6,8,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,14,18	2,4,6,8,13,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,7,10,14,16,17	2,4,6,8,13,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0)$	1,3,5,7,10,14	2,4,6,8,13,15	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0)$	1,3,5,7,10,14,16,17,18	2,4,6,8,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,7,10,12	2,4,6,8	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,7,10,12,16,17,18	2,4,6,8,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0)$	1,3,5,7,10,12,18	2,4,6,8,15,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0)$	1,3,5,7,10,12,16,17	2,4,6,8,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,7,10,12,14,17,18	2,4,6,8,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,7,10,12,14,16	2,4,6,8	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1)$	1,3,5,7,10,12,14,17	2,4,6,8,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1)$	1,3,5,7,10,12,14,16,18	2,4,6,8,15,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,7,10,12,18	2,4,6,8,13,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,7,10,12,16,17	2,4,6,8,13,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)$	1,3,5,7,10,12	2,4,6,8,13,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0)$	1,3,5,7,10,12,16,17,18	2,4,6,8,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,7,10,12,14,17	2,4,6,8,13,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,7,10,12,14,16,18	2,4,6,8,13,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1)$	1,3,5,7,10,12,14,17,18	2,4,6,8,13,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1)$	1,3,5,7,10,12,14,16	2,4,6,8,13,15	$2^{-6.5}$

Table 0.2044 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,7,10,17	2,4,6,8,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,7,10,16,18	2,4,6,8,11,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1)$	1,3,5,7,10,17,18	2,4,6,8,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)$	1,3,5,7,10,16	2,4,6,8,11,15	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7,10,14,18	2,4,6,8,11,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,7,10,14,16,17	2,4,6,8,11,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0)$	1,3,5,7,10,14	2,4,6,8,11,15	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0)$	1,3,5,7,10,14,16,17,18	2,4,6,8,11,15,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,7,10,17,18	2,4,6,8,11,13,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,7,10,16	2,4,6,8,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1)$	1,3,5,7,10,17	2,4,6,8,11,13,15,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1)$	1,3,5,7,10,16,18	2,4,6,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,7,10,14	2,4,6,8,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,7,10,14,16,17,18	2,4,6,8,11,13,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0)$	1,3,5,7,10,14,18	2,4,6,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0)$	1,3,5,7,10,14,16,17	2,4,6,8,11,13,15,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,7,10,12,18	2,4,6,8,11,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,7,10,12,16,17	2,4,6,8,11,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 0)$	1,3,5,7,10,12	2,4,6,8,11,15	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 0)$	1,3,5,7,10,12,16,17,18	2,4,6,8,11,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,7,10,12,14,17	2,4,6,8,11,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,7,10,12,14,16,18	2,4,6,8,11,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1)$	1,3,5,7,10,12,14,17,18	2,4,6,8,11,15,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1)$	1,3,5,7,10,12,14,16	2,4,6,8,11,15	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,7,10,12	2,4,6,8,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,7,10,12,16,17,18	2,4,6,8,11,13,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0)$	1,3,5,7,10,12,18	2,4,6,8,11,13,15,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0)$	1,3,5,7,10,12,16,17	2,4,6,8,11,13,15,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,7,10,12,14,17,18	2,4,6,8,11,13,17,18	2^{-34}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,7,10,12,14,16	2,4,6,8,11,13	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1)$	1,3,5,7,10,12,14,17	2,4,6,8,11,13,15,17	2^{-34}
$(1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,7,10,12,14,16,18	2,4,6,8,11,13,15,18	$2^{-17.5}$

Table 0.2045 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,7,18	2,4,6,8,9,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,7,16,17	2,4,6,8,9,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0)$	1,3,5,7	2,4,6,8,9,15	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0)$	1,3,5,7,16,17,18	2,4,6,8,9,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,7,14,17	2,4,6,8,9,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,7,14,16,18	2,4,6,8,9,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1)$	1,3,5,7,14,17,18	2,4,6,8,9,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 1)$	1,3,5,7,14,16	2,4,6,8,9,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,7	2,4,6,8,9,13	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,7,16,17,18	2,4,6,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 0)$	1,3,5,7,18	2,4,6,8,9,13,15,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,7,16,17	2,4,6,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,7,14,17,18	2,4,6,8,9,13,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,7,14,16	2,4,6,8,9,13	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1)$	1,3,5,7,14,17	2,4,6,8,9,13,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1)$	1,3,5,7,14,16,18	2,4,6,8,9,13,15,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,7,12,17	2,4,6,8,9,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,12,16,18	2,4,6,8,9,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1)$	1,3,5,7,12,17,18	2,4,6,8,9,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1)$	1,3,5,7,12,16	2,4,6,8,9,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,12,14,18	2,4,6,8,9,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0)$	1,3,5,7,12,14,16,17	2,4,6,8,9,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0)$	1,3,5,7,12,14	2,4,6,8,9,15	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0)$	1,3,5,7,12,14,16,17,18	2,4,6,8,9,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,7,12,17,18	2,4,6,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,7,12,16	2,4,6,8,9,13	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1)$	1,3,5,7,12,17	2,4,6,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1)$	1,3,5,7,12,16,18	2,4,6,8,9,13,15,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,7,12,14	2,4,6,8,9,13	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,7,12,14,16,17,18	2,4,6,8,9,13,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)$	1,3,5,7,12,14,18	2,4,6,8,9,13,15,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0)$	1,3,5,7,12,14,16,17	2,4,6,8,9,13,15,17	$2^{-6.5}$

Table 0.2046 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bi
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,7	2,4,6,8,9,11	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,7,16,17,18	2,4,6,8,9,11,17,18	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,7,18	2,4,6,8,9,11,15,18	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0)$	1,3,5,7,16,17	2,4,6,8,9,11,15,17	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,7,14,17,18	2,4,6,8,9,11,17,18	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,7,14,16	2,4,6,8,9,11	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1)$	1,3,5,7,14,17	2,4,6,8,9,11,15,17	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1)$	1,3,5,7,14,16,18	2,4,6,8,9,11,15,18	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,7,18	2,4,6,8,9,11,13,18	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,7,16,17	2,4,6,8,9,11,13,17	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0)$	1,3,5,7	2,4,6,8,9,11,13,15	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0)$	1,3,5,7,16,17,18	2,4,6,8,9,11,13,15,17,18	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,7,14,17	2,4,6,8,9,11,13,17	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,7,14,16,18	2,4,6,8,9,11,13,18	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$	1,3,5,7,14,17,18	2,4,6,8,9,11,13,15,17,18	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1)$	1,3,5,7,14,16	2,4,6,8,9,11,13,15	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,7,12,17,18	2,4,6,8,9,11,17,18	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,7,12,16	2,4,6,8,9,11	2^{-2}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1)$	1,3,5,7,12,17	2,4,6,8,9,11,15,17	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1)$	1,3,5,7,12,16,18	2,4,6,8,9,11,15,18	2^{-2}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,7,12,14	2,4,6,8,9,11	2^{-2}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,7,12,14,16,17,18	2,4,6,8,9,11,17,18	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0)$	1,3,5,7,12,14,18	2,4,6,8,9,11,15,18	2^{-2}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$	1,3,5,7,12,14,16,17	2,4,6,8,9,11,15,17	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,7,12,17	2,4,6,8,9,11,13,17	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,7,12,16,18	2,4,6,8,9,11,13,18	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1)$	1,3,5,7,12,17,18	2,4,6,8,9,11,13,15,17,18	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1)$	1,3,5,7,12,16	2,4,6,8,9,11,13,15	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1)$	1,3,5,7,12,14,18	2,4,6,8,9,11,13,18	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,12,14,16,17	2,4,6,8,9,11,13,17	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0)$	1,3,5,7,12,14	2,4,6,8,9,11,13,15	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0)$	1,3,5,7,12,14,16,17,18	2,4,6,8,9,11,13,15,17,18	2^{-1}

Table 0.2047 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bias
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,7,10,17	2,4,6,8,9,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,7,10,16,18	2,4,6,8,9,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1)$	1,3,5,7,10,17,18	2,4,6,8,9,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)$	1,3,5,7,10,16	2,4,6,8,9,15	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,7,10,14,18	2,4,6,8,9,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,7,10,14,16,17	2,4,6,8,9,17	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,7,10,14	2,4,6,8,9,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 0)$	1,3,5,7,10,14,16,17,18	2,4,6,8,9,15,17,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,7,10,17,18	2,4,6,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,7,10,16	2,4,6,8,9,13	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1)$	1,3,5,7,10,17	2,4,6,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1)$	1,3,5,7,10,16,18	2,4,6,8,9,13,15,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,7,10,14	2,4,6,8,9,13	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,7,10,14,16,17,18	2,4,6,8,9,13,17,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 0)$	1,3,5,7,10,14,18	2,4,6,8,9,13,15,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0)$	1,3,5,7,10,14,16,17	2,4,6,8,9,13,15,17	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0)$	1,3,5,7,10,12,18	2,4,6,8,9,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,7,10,12,16,17	2,4,6,8,9,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0)$	1,3,5,7,10,12	2,4,6,8,9,15	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0)$	1,3,5,7,10,12,16,17,18	2,4,6,8,9,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,7,10,12,14,17	2,4,6,8,9,17	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,7,10,12,14,16,18	2,4,6,8,9,18	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1)$	1,3,5,7,10,12,14,17,18	2,4,6,8,9,15,17,18	2^{-23}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1)$	1,3,5,7,10,12,14,16	2,4,6,8,9,15	$2^{-6.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0)$	1,3,5,7,10,12	2,4,6,8,9,13	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,7,10,12,16,17,18	2,4,6,8,9,13,17,18	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0)$	1,3,5,7,10,12,18	2,4,6,8,9,13,15,18	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0)$	1,3,5,7,10,12,16,17	2,4,6,8,9,13,15,17	$2^{-17.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,7,10,12,14,17,18	2,4,6,8,9,13,17,18	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,7,10,12,14,16	2,4,6,8,9,13	2^{-12}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1)$	1,3,5,7,10,12,14,17	2,4,6,8,9,13,15,17	$2^{-28.5}$
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1)$	1,3,5,7,10,12,14,16,18	2,4,6,8,9,13,15,18	2^{-12}

Table 0.2048 Nontrivial 1-round linear relations for MESH-128(8).

1-round linear relation	Weak subkeys $Z_j^{(i)}$		Bi
	j values (i odd)	j values (i even)	
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,7,10,17,18	2,4,6,8,9,11,17,18	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,7,10,16	2,4,6,8,9,11	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$	1,3,5,7,10,17	2,4,6,8,9,11,15,17	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1)$	1,3,5,7,10,16,18	2,4,6,8,9,11,15,18	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,7,10,14	2,4,6,8,9,11	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,7,10,14,16,17,18	2,4,6,8,9,11,17,18	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0)$	1,3,5,7,10,14,18	2,4,6,8,9,11,15,18	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0)$	1,3,5,7,10,14,16,17	2,4,6,8,9,11,15,17	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,7,10,17	2,4,6,8,9,11,13,17	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,7,10,16,18	2,4,6,8,9,11,13,18	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1)$	1,3,5,7,10,17,18	2,4,6,8,9,11,13,15,17,18	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1)$	1,3,5,7,10,16	2,4,6,8,9,11,13,15	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7,10,14,18	2,4,6,8,9,11,13,18	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,7,10,14,16,17	2,4,6,8,9,11,13,17	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0)$	1,3,5,7,10,14	2,4,6,8,9,11,13,15	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0)$	1,3,5,7,10,14,16,17,18	2,4,6,8,9,11,13,15,17,18	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,7,10,12	2,4,6,8,9,11	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,7,10,12,16,17,18	2,4,6,8,9,11,17,18	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0)$	1,3,5,7,10,12,18	2,4,6,8,9,11,15,18	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0)$	1,3,5,7,10,12,16,17	2,4,6,8,9,11,15,17	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,7,10,12,14,17,18	2,4,6,8,9,11,17,18	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,7,10,12,14,16	2,4,6,8,9,11	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1)$	1,3,5,7,10,12,14,17	2,4,6,8,9,11,15,17	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1)$	1,3,5,7,10,12,14,16,18	2,4,6,8,9,11,15,18	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0) \xrightarrow{1r} (0, 0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,7,10,12,18	2,4,6,8,9,11,13,18	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0, 1) \xrightarrow{1r} (1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,7,10,12,16,17	2,4,6,8,9,11,13,17	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0) \xrightarrow{1r} (1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0)$	1,3,5,7,10,12	2,4,6,8,9,11,13,15	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 1) \xrightarrow{1r} (0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$	1,3,5,7,10,12,16,17,18	2,4,6,8,9,11,13,15,17,18	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 0) \xrightarrow{1r} (1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,7,10,12,14,17	2,4,6,8,9,11,13,17	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1) \xrightarrow{1r} (0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,7,10,12,14,16,18	2,4,6,8,9,11,13,18	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 0) \xrightarrow{1r} (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$	1,3,5,7,10,12,14,17,18	2,4,6,8,9,11,13,15,17,18	2^{-1}
$(1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1) \xrightarrow{1r} (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$	1,3,5,7,10,12,14,16	2,4,6,8,9,11,13,15	2^{-1}